

M208

Pure mathematics

Book B

Group theory 1

This publication forms part of an Open University module. Details of this and other Open University modules can be obtained from Student Recruitment, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)300 303 5303; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2018.

Copyright © 2018 The Open University

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Barnard's Inn, 86 Fetter Lane, London EC4A 1EN (website www.cla.co.uk).

Open University materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or retransmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using L^AT_EX.

Printed in the United Kingdom by Hobbs the Printers Limited, Brunel Road, Totton, Hampshire, SO40 3WX.

Contents

Unit B1 Symmetry and groups	1
Introduction to Book B	3
Introduction	4
1 Symmetry in \mathbb{R}^2	4
1.1 Symmetries of plane figures	4
1.2 Four properties of the set of symmetries of a plane figure	11
1.3 Symmetries of the disc	18
1.4 Direct and indirect symmetries	20
2 Representing symmetries	23
2.1 Two-line symbols	23
2.2 Composing and inverting symmetries in two-line notation	27
2.3 Cayley tables	30
3 Definition of a group	33
3.1 The group axioms	33
3.2 Checking the group axioms	36
3.3 Checking the group axioms for small finite sets	46
3.4 Standard groups of numbers	55
4 Deductions from the group axioms	58
4.1 Basic properties of groups	59
4.2 Properties of group tables	66
5 Symmetry in \mathbb{R}^3	70
5.1 Symmetries of figures in \mathbb{R}^3	70
5.2 Counting the symmetries of a polyhedron	76
5.3 Finding the symmetries of a polyhedron	84
5.4 The Platonic solids	88
Summary	89
Learning outcomes	90
Solutions to exercises	91

Unit B2	Subgroups and isomorphisms	105
	Introduction	107
1	Subgroups	107
1.1	What is a subgroup?	107
1.2	Checking whether a subset forms a subgroup	111
1.3	Subgroups of symmetry groups	122
2	Order of a group element	128
2.1	Powers of a group element	128
2.2	What is the order of a group element?	133
2.3	Finding the orders of group elements	138
3	Cyclic subgroups and cyclic groups	141
3.1	The subgroup generated by an element	141
3.2	Cyclic groups	148
3.3	Cyclic groups from modular arithmetic	153
3.4	The group $(\mathbb{Z}_n, +_n)$	155
4	Isomorphisms	161
4.1	Cayley tables of groups of orders 4 and 6	161
4.2	Isomorphic groups	167
4.3	Properties of isomorphisms	175
4.4	Isomorphisms of cyclic groups	182
	Summary	186
	Learning outcomes	186
	Solutions to exercises	187

Unit B3	Permutations	203
	Introduction	205
1	Permutations	205
1.1	Cycle form of a permutation	205
1.2	Composing permutations	212
1.3	Finding the inverse of a permutation	217
2	Permutation groups	219
2.1	The symmetric group S_n	219
2.2	Cycle structure	222
2.3	Order of a permutation	224
2.4	Representing symmetries as permutations	227
3	Even and odd permutations	236
3.1	Expressing a permutation as a composite of transpositions	236
3.2	Parity of a permutation	240
3.3	The alternating group A_n	244
3.4	Proof of the Parity Theorem (optional)	247
4	Conjugacy in S_n	250
4.1	Conjugate permutations in S_n	250
4.2	Conjugate subgroups in S_n	257
5	Subgroups of S_4	261
6	Cayley's Theorem	268
	Summary	276
	Learning outcomes	276
	Solutions to exercises	277

Unit B4 Lagrange's Theorem and small groups	291
Introduction	293
1 Lagrange's Theorem	293
1.1 Orders of subgroups of a group	293
1.2 Corollaries of Lagrange's Theorem	300
2 Groups of small order	303
2.1 Some useful results	303
2.2 Groups of orders 1, 2, 3, 5 and 7	307
2.3 Groups of order 4	308
2.4 Groups of order 6	309
2.5 Groups of order 8	313
2.6 Summary of isomorphism classes for groups of orders 1 to 8	318
3 Theorems and proofs in group theory	319
3.1 Statements of theorems	319
3.2 Producing proofs	329
3.3 Proofs using the group axioms	330
3.4 Proofs involving subgroups	337
3.5 Checking proofs	342
Summary	347
Learning outcomes	347
Solutions to exercises	348
Acknowledgements	359
Index	361

Unit B1

Symmetry and groups

Introduction to Book B

In this book and Book E you will study a branch of mathematics known as *group theory*. The word *group* describes a particular type of mathematical structure that occurs naturally in many branches of mathematics, as well as in other disciplines such as chemistry and physics. In particular, this structure is to be found wherever *symmetry* exists. Figure 1 illustrates some of the many ways in which symmetry occurs in nature: for example, the human form is (outwardly) symmetric, as are many biological, chemical and geological forms.

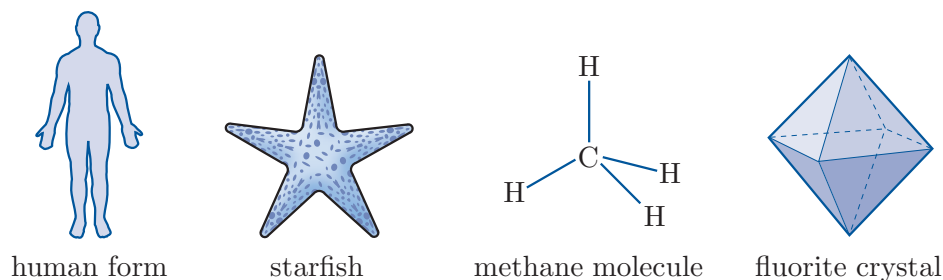


Figure 1 Symmetry in nature

You will see how groups arise from symmetry, and how they occur in other contexts, such as in relation to addition and multiplication of numbers. You will study the theory of groups, which allows us to discover and make use of the properties of groups that arise from their structure, rather than from the nature of the actual objects that form the group – these objects might be numbers, or functions, or any of many other possibilities. You will see how group theory, a rich and beautiful mathematical theory, is built up from just four simple assumptions about the nature of the structure that we call a group; these assumptions are known as the *group axioms*.

This first book of group theory introduces the basic ideas leading up to a simple but powerful result known as *Lagrange's Theorem*, which underpins much of the development of the subject. The second book of group theory, Book E, takes the theory further. Although you will be learning abstract theory throughout the group theory books, you will also encounter many concrete examples of groups and see how these illustrate the abstract ideas.

The first two units in Book B, namely Unit B1 *Symmetry and groups* and Unit B2 *Subgroups and isomorphisms*, are quite substantial, and you should expect to spend longer studying them than you would for an average unit, particularly for Unit B1. In compensation, Unit B3 *Permutations* and Unit B4 *Lagrange's Theorem and small groups* are shorter.

A note about proofs

In this book, and throughout the rest of this module, you will see many proofs. You have seen some already in previous units, but the number of proofs will increase from now on.

These proofs are important: proofs are an essential part of mathematics. If you take the time to read and understand them, then they will often improve your understanding of the theory, and they will also help you to learn how to write your own proofs, which you are asked to do in some exercises.

However, some proofs can be difficult and time-consuming to read. Also, sometimes a proof may not contribute significantly to your understanding of the theory: for example, it might mostly depend on ideas that are not closely connected to the mathematics that you are currently studying, or it might consist of a largely technical and not very enlightening check through various possible cases. It may be better for you to skip such proofs, at least initially, especially if you are short of time or if you do not plan to go on to study more pure mathematics after M208. Throughout the module, the unit texts provide guidance about some proofs that you might choose to skip or delay reading for these reasons.

Introduction

In this first unit of group theory you will look at ideas of symmetry for two- and three-dimensional shapes, and see how these ideas can be expressed mathematically. You will see how this leads to the concept of a group, and you will meet many other examples of groups. You will also see how some simple results about groups can be deduced directly from the group axioms.

Remember that this is quite a substantial unit, so you should expect it to take more time than an average unit.

1 Symmetry in \mathbb{R}^2

This first section is about the symmetry of two-dimensional shapes.

1.1 Symmetries of plane figures

When you think of symmetry, you probably think of shapes like the heart shape in Figure 2: it has *reflectional symmetry* because a reflection in its *axis of symmetry* leaves the shape looking the same. Another type of symmetry is exhibited by the capital N also shown in Figure 2: it has *rotational symmetry* because a rotation of a half-turn about its centre leaves the shape looking the same. For other shapes, rotational symmetry may involve a quarter-turn or a third of a turn, for example.

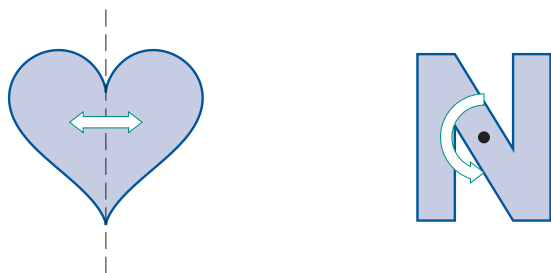


Figure 2 A heart shape and a capital N

Both types of symmetry, reflectional and rotational, are described in terms of transformations that leave a shape as a whole looking the same, namely reflections and rotations. These types of transformations can be used to describe symmetry because they transform shapes *rigidly* – that is, without distorting their size or shape. In other words, they *preserve distances* between points: the distance between any two points is the same as the distance between their images under the transformation. Transformations that have this property are known as *isometries*.

To enable us to formalise these ideas about symmetry, we make the following definitions. You have met the first definition below already, in Unit A1 *Sets, functions and vectors*.

Definitions

A **plane figure** is any subset of the plane \mathbb{R}^2 .

A **bounded** plane figure is one that can be surrounded by a circle (of finite radius).

For example, the heart shape and the capital N in Figure 2 are bounded plane figures. An infinitely long straight line is a plane figure, but not a bounded plane figure. In the group theory books of this module, we will mainly consider plane figures that are bounded.

We define a *symmetry* of a plane figure as an isometry that maps the figure to itself, as follows, and as illustrated in Figure 3.

Definitions

An **isometry** of the plane is a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ that preserves distances; that is, for all points $X, Y \in \mathbb{R}^2$, the distance between $f(X)$ and $f(Y)$ is the same as the distance between X and Y .

A **symmetry** of a plane figure F is an isometry that maps F to itself, that is, an isometry $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ such that $f(F) = F$.

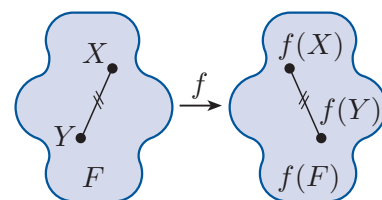


Figure 3 An isometry f preserves distances

As you may have learned in your previous studies, the isometries of the plane are of four types: *rotations*, *reflections*, *translations* and *glide-reflections*. A **rotation** rotates each point of the plane through the same angle about a particular point. A **reflection** reflects each point of the plane in a particular line. A **translation** moves each point of the plane by the same distance in the same direction. A **glide-reflection** is a reflection in a line followed by a translation parallel to that line.

For a *bounded* plane figure, such as the heart shape, any translation (except the translation through zero distance) does not map the figure to itself and so is not a symmetry. The same is true of a glide-reflection (unless the translation involved is the zero translation – in which case the glide-reflection is simply a reflection). So the types of isometries that are potential symmetries of a bounded plane figure are the following.

- The **identity transformation**: equivalent to doing nothing to a figure.
- A **rotation**: specified by a *centre* and an *angle of rotation*, as illustrated in Figure 4(a).
- A **reflection**: specified by a line – an *axis of symmetry*, as illustrated in Figure 4(b).

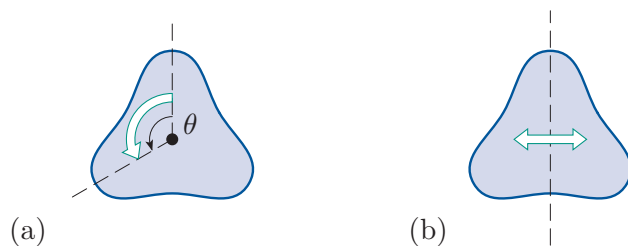


Figure 4 (a) A rotation about a centre through an angle θ (b) A reflection in an axis of symmetry

The identity transformation can be regarded as a zero rotation or a zero translation. We refer to it as the **identity symmetry** of a figure, or just the **identity**. It is sometimes called the **trivial symmetry**.

A **rotational symmetry** is a symmetry that is a rotation, and a **reflectional symmetry** is a symmetry that is a reflection.

When specifying a rotational symmetry, we measure angles anticlockwise, as illustrated in Figure 4(a) (unless otherwise stated), and interpret negative angles as clockwise. The angle $2\pi/3$, for example, specifies an anticlockwise rotation through $2\pi/3$ radians, whereas $-2\pi/3$ specifies a clockwise rotation through $2\pi/3$ radians.

All the rotational symmetries of a *bounded* plane figure have the same centre of rotation (except that the identity symmetry can be regarded as a rotation about any point), and all the axes of symmetry of the figure pass through this centre, as illustrated in Figure 5.

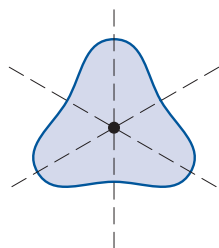


Figure 5 The centre of rotational symmetry and axes of symmetry of a bounded plane figure

Of course, some figures, such as the one in Figure 6, have no symmetries other than the identity symmetry.

Since a rotation through 2π radians has the same effect on a figure as the identity symmetry, we consider these two transformations to be the same. In general, we have the following definition.

Definition

Two symmetries f and g of a figure F are **equal** if they have the same effect on F , that is, $f(X) = g(X)$ for all points $X \in F$.

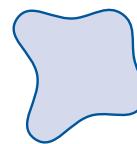


Figure 6 An irregular figure

The rotation through 0 radians is called the **trivial rotation**; it is equal to the identity symmetry. Any rotation not equal to the trivial rotation is called a **non-trivial rotation**.

We can apply our ideas of symmetry to any plane figure, but we will mainly consider the regular polygons, the first few of which are shown in Figure 7. In general, a **polygon** is a bounded plane figure with straight edges, and a **regular polygon** is a polygon all of whose edges have the same length and all of whose angles are equal.

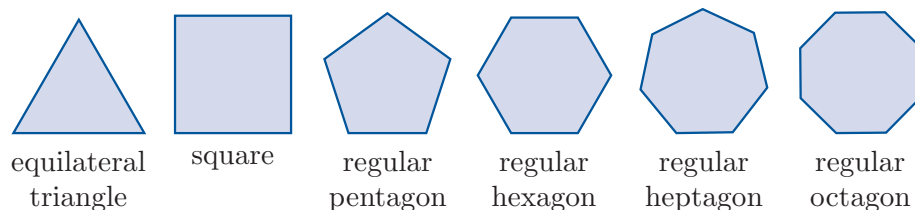


Figure 7 Regular polygons

Let us illustrate the ideas by starting with the square. Remember that we consider the square to be a subset of the plane, with its four vertices located at definite positions in \mathbb{R}^2 . We need a means of tracking the position of the square relative to its initial position after a rotation or a reflection has been carried out.

To do this, imagine a paper model of the square that we can move around in the plane. If we mark a dot in one corner of this paper model, then we can keep track of the position of the square after a rotation. For example, if we take the initial position of the square to be as shown in Figure 8(a), with the dot in the top left corner, then after the square has been rotated anticlockwise through a quarter turn, its position is as shown in Figure 8(b), with the dot in the bottom left corner.



Figure 8 The position of the square (a) initially (b) after it has been rotated through a quarter turn anticlockwise

Using our paper model to keep track of the position of the square after a reflection is not quite so easy. A reflection takes each point of the square to its mirror-image in an axis of symmetry. This is not something we can demonstrate with our paper model by moving it around within the plane.

However, we achieve the same *effect* as a reflection if we ‘flip’ the paper square along the axis of symmetry. Turning the paper square over in this way takes each point of the square to its mirror-image in the axis of symmetry, just as the reflection does. Therefore, if we colour the two sides of the paper square differently – say, light blue on one side and darker blue on the other – and mark the dot in the same corner on both sides (as if the dot goes through the paper), then we can keep track of the position of the square after a reflection.

For example, if we again take the initial position of the square to be as shown in Figure 9(a), with the dot in the top left corner and the light blue side showing, then after the square has been reflected in the vertical axis of symmetry its position is as shown in Figure 9(b), with the darker side showing and the dot in the top right corner.



Figure 9 The position of the square (a) initially (b) after it has been reflected in the vertical axis of symmetry

We now use this paper model to describe the symmetries of the square. You might find it helpful to make such a model.

The square has four rotational symmetries, namely the rotations about its centre through 0 , $\pi/2$, π and $3\pi/2$ radians (anticlockwise), since all of these transformations map the square to itself, as shown in Figure 10. The rotation through 0 radians is just the identity symmetry.

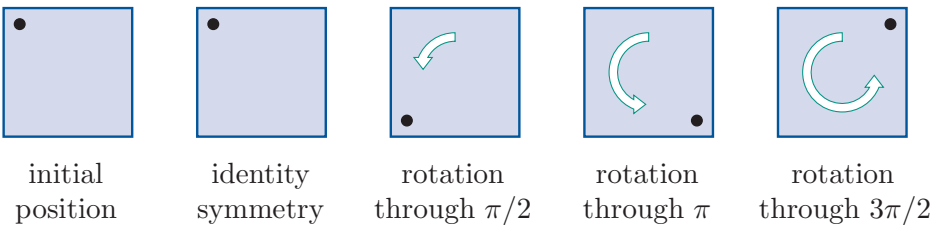


Figure 10 The four rotational symmetries of the square

A rotation through 2π radians returns the square to its original position, and so is the same symmetry as the identity symmetry. Similarly, a rotation through $5\pi/2$ radians is the same symmetry as a rotation through $\pi/2$ radians, because its overall effect on the square is the same. A rotation through $-\pi/2$ radians is the same symmetry as a rotation through $3\pi/2$ radians, because a rotation through $\pi/2$ radians clockwise has the same effect on the square as a rotation through $3\pi/2$ radians anticlockwise.

Now let us consider the reflectional symmetries of the square. The square has four axes of symmetry: a vertical axis, a horizontal axis and two diagonal axes. So it has four reflectional symmetries, as shown in Figure 11.

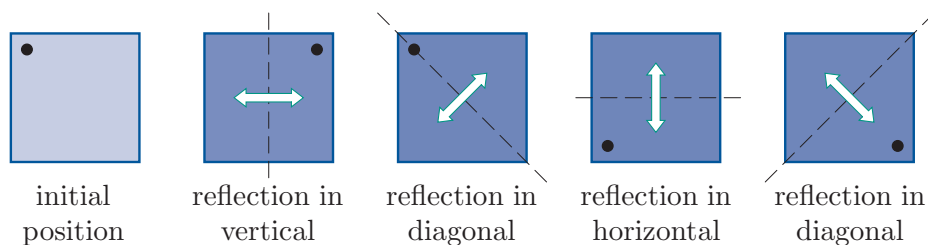


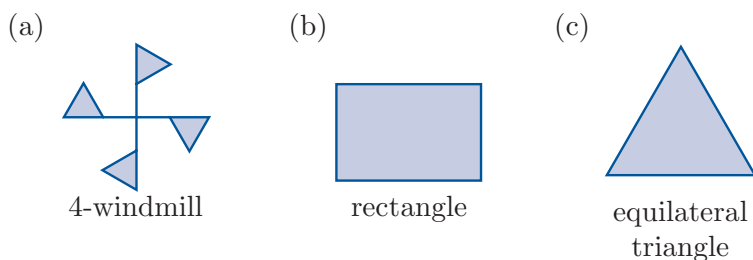
Figure 11 The four reflectional symmetries of the square

This completes the set of symmetries of the square. It contains eight elements: the identity, three non-trivial rotations and four reflections.

In the next exercise you are asked to find the symmetries of three more plane figures, namely the *4-windmill* (a symmetric windmill shape with four ‘sails’), the rectangle and the equilateral triangle.

Exercise B1

For each of the following figures, describe its set of symmetries by drawing diagrams similar to those given in Figures 10 and 11 for the square.



(To hand-draw the light and dark sides of the models reasonably quickly, you could draw them in the way illustrated for the square in Figure 12.)

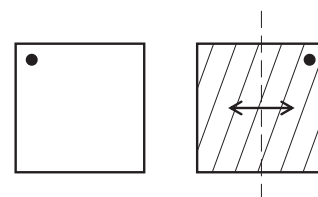


Figure 12 Hand-drawing the paper model of the square

Symmetries of a regular polygon

You saw in Exercise B1(c) that an equilateral triangle has six symmetries: three rotations and three reflections, as shown in Figure 13(a) (recall that we may think of the identity symmetry as a rotation). You have also seen that a square has eight symmetries: four rotations and four reflections, as shown in Figure 13(b).

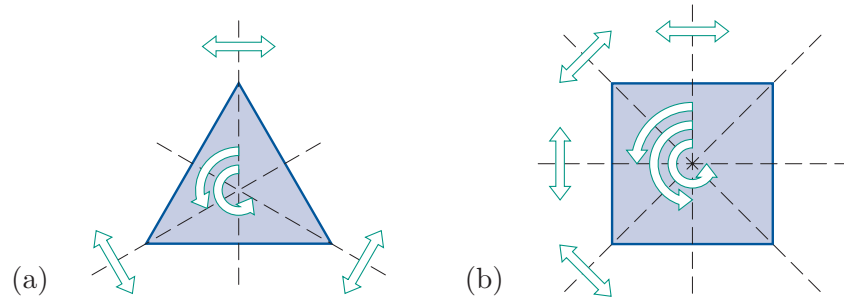


Figure 13 The symmetries of the equilateral triangle and the square (the identity symmetry is not shown)

These are special cases of the following general fact.

A regular polygon with n edges has $2n$ symmetries, namely n rotations (through multiples of $2\pi/n$) and n reflections.

These symmetries are illustrated in Figure 14. A regular polygon with n edges is known as a **regular n -gon**.

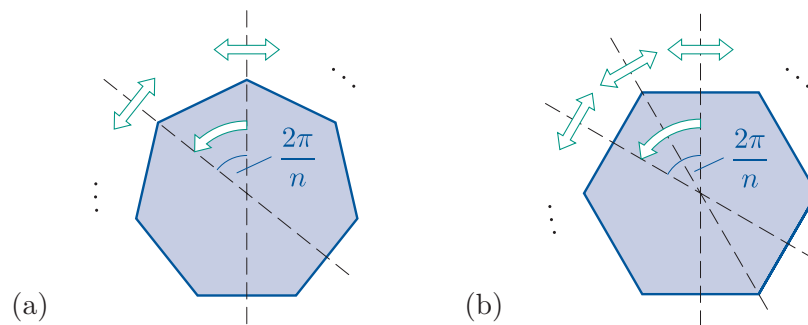


Figure 14 Symmetries of a regular n -gon (a) when n is odd (b) when n is even

For odd values of n , each of the n axes of symmetry passes through a vertex and the midpoint of the opposite edge, as shown in Figure 14(a).

For even values of n , there are $n/2$ axes of symmetry that pass through opposite vertices and $n/2$ axes of symmetry that pass through the midpoints of opposite edges, as shown in Figure 14(b).

1.2 Four properties of the set of symmetries of a plane figure

For any plane figure F , we denote the set of all symmetries of F by $S(F)$. Every figure F has at least one symmetry, namely the identity symmetry, usually denoted by e . So, for every plane figure F , the set $S(F)$ of symmetries of F is non-empty.

In this subsection, you will meet four important properties that the set $S(F)$ always has, no matter what the figure F is.

Closure

Let F be any plane figure. As you saw in the last subsection, the elements of $S(F)$ are the distance-preserving functions $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ such that $f(F) = F$. Suppose that f and g are elements of $S(F)$. Then we can form the composite function $g \circ f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$. (Remember that \circ is read simply as ‘circle’.) Since f and g both preserve distance, so must $g \circ f$; and since f and g both map F to itself, so must $g \circ f$, as illustrated in Figure 15. Hence $g \circ f$ is also an element of $S(F)$. So we know that if f and g are elements of $S(F)$, then $g \circ f$ is an element of $S(F)$. We describe this situation by saying that the set $S(F)$ is *closed* under composition of functions. This is our first important property, stated as a proposition in the box below.

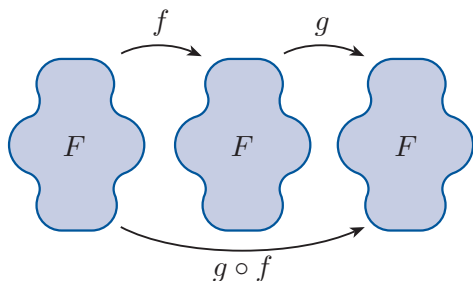


Figure 15 If f and g are symmetries of a plane figure F , then so is $g \circ f$

Proposition B1 Closure property for symmetries

The set of symmetries $S(F)$ of a plane figure F is **closed** under composition of functions; that is, for all elements f and g of $S(F)$, the composite $g \circ f$ is an element of $S(F)$.

So if we take any two symmetries of a plane figure and compose them, then we can recognise the result as a symmetry of the figure.

To illustrate this, let us compose some elements of $S(\square)$, the set of symmetries of the square. (The notation $S(\square)$ is read as ‘S square’.)

Figure 16 shows the symmetries of the square, which were described in the previous subsection, and it introduces a labelling for these symmetries that we will use throughout the group theory books of this module. The identity symmetry, which is not shown in Figure 16, is denoted by e , as usual.

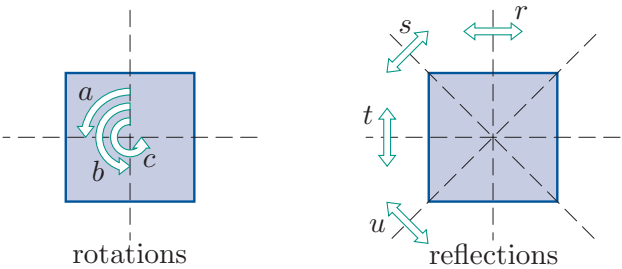


Figure 16 Standard labelling for the elements of $S(\square)$

We will be using the labelling in Figure 16 frequently, so you will probably find it useful to try to remember it. The non-trivial rotations are a , b and c , in order of the angle of rotation, and the reflections are r , s , t and u , starting from the vertical axis of symmetry and working anticlockwise. We will use a similar labelling convention for the symmetries of some of the other regular polygons.

Note that the axes of symmetry of the square are fixed in the plane; so, for example, r means ‘reflect in the vertical axis of symmetry, regardless of any symmetries already carried out’. The worked exercise below should clarify what this statement means in practice.

Worked Exercise B1

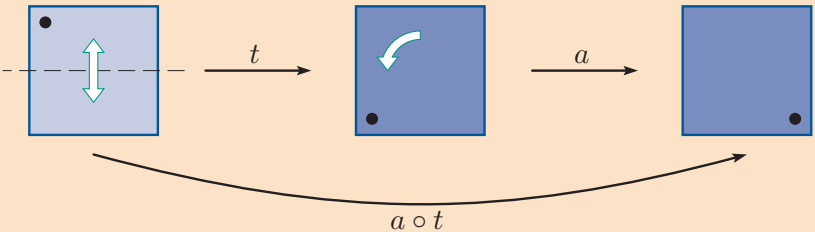
Find the following composites of symmetries of the square.

- (a) $a \circ t$ (b) $t \circ a$

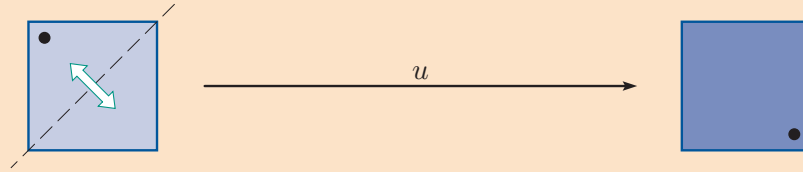
Solution

To keep track of composing the symmetries, we draw pictures of the paper model of the square described earlier, with light and dark sides and a dot in the corner. The starting position is always with the light side showing and the dot in the top left corner.

- (a) We draw the effect of applying $a \circ t$, that is, first t and then a , to the starting position of the square.



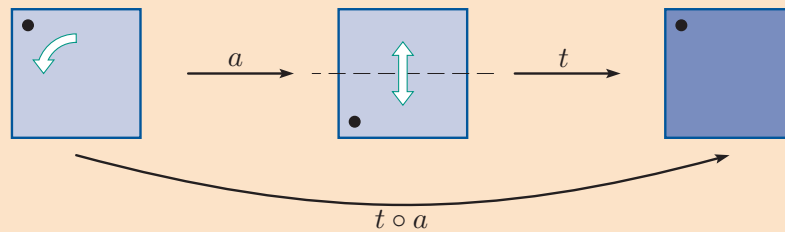
Looking at the final position, we see that the effect of $a \circ t$ is to reflect the square in the diagonal from bottom left to top right, as shown below. This is the same as the effect of the symmetry u .



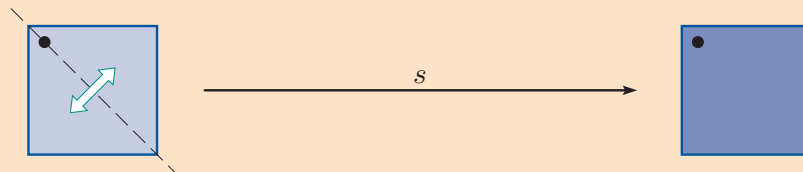
The diagrams show that

$$a \circ t = u.$$

- (b) We proceed as in part (a). We draw the effect of $t \circ a$, that is, first a and then t .



We see that the effect of $t \circ a$ is the same as the effect of s .



The diagrams show that

$$t \circ a = s.$$

Notice that in the worked exercise above, $t \circ a \neq a \circ t$.

Here is a similar exercise for you to try.

Exercise B2

Find the following composites of symmetries of the square. (The labelling of the symmetries, introduced in Figure 16, is summarised in Figure 17 for easy reference.)

- (a) $b \circ c$ (b) $s \circ s$ (c) $t \circ u$

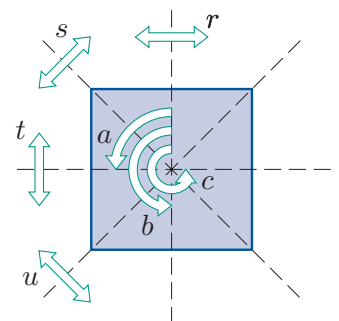


Figure 17 $S(\square)$

Worked Exercise B1 and Exercise B2 illustrate a number of properties of composition of symmetries of a figure F , as follows.

First, order of composition is important. For example, in Worked Exercise B1 you saw that

$$a \circ t = u$$

but

$$t \circ a = s.$$

In general, if $f, g \in S(F)$, then $g \circ f$ may or may not be equal to $f \circ g$. That is, in general, composition of symmetries is not *commutative*.

Second, composition of rotational and reflectional symmetries of a bounded plane figure follows a standard pattern, as follows:

- rotation \circ rotation = rotation,
- rotation \circ reflection = reflection,
- reflection \circ rotation = reflection,
- reflection \circ reflection = rotation.

For example, in $S(\square)$,

$$b \circ c = a, \quad a \circ t = u, \quad t \circ a = s, \quad t \circ u = c.$$

The pattern above is summarised in the following table:

\circ	rotation	reflection
rotation	rotation	reflection
reflection	reflection	rotation

Finally, composing a reflection with itself gives the identity symmetry e .

For example, in $S(\square)$,

$$r \circ r = e, \quad s \circ s = e, \quad t \circ t = e, \quad u \circ u = e.$$

This should be no surprise! If you reflect twice in the same axis then you get back to where you started.

The next exercise is about composing the symmetries of the three plane figures whose symmetries you were asked to find in Exercise B1, namely the 4-windmill, the rectangle and the equilateral triangle. These three shapes are shown in Figure 18, along with the standard labelling that we will use for their symmetries. In each case the identity symmetry is not shown but is denoted by e , as usual.

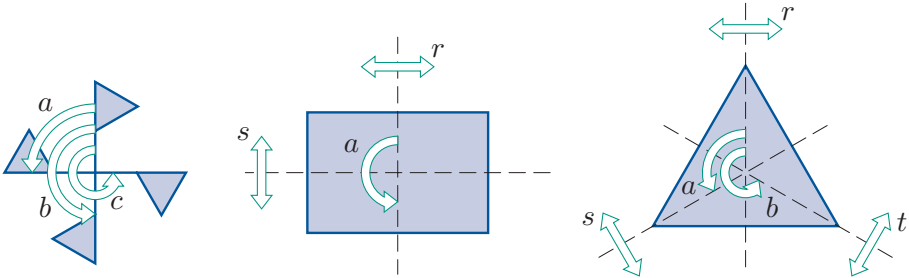


Figure 18 Standard labelling for the elements of $S(\text{4-windmill})$, $S(\square)$ and $S(\triangle)$

Exercise B3

- (a) For the 4-windmill, find the following composites of symmetries.
 (i) $a \circ b$ (ii) $a \circ c$
- (b) For the rectangle, find the following composites of symmetries.
 (i) $a \circ r$ (ii) $a \circ s$ (iii) $r \circ s$
- (c) For the equilateral triangle, find the following composites of symmetries.
 (i) $a \circ b$ (ii) $a \circ r$ (iii) $s \circ t$

Associativity

We now move on to a second important property of the set of symmetries of a figure F . This property is called *associativity*, and it is a general property of composition of functions.

To illustrate it, let us look at an example of composing *three* elements of $S(\square)$, the set of symmetries of the square (see Figure 19). If we want to compose the elements t , a and b , in that order, then we can first compose t with a , and then compose the result with b :

$$b \circ (a \circ t) = b \circ u = s.$$

(Remember that $a \circ t$ means ‘do t , then a ’. You saw that $a \circ t = u$ in Worked Exercise B1, and you can work out that $b \circ u = s$ using the same method.)

Alternatively, we can first compose a with b and then compose t with the result:

$$(b \circ a) \circ t = c \circ t = s.$$

(You can work out that $b \circ a = c$ and $c \circ t = s$ using the method of Worked Exercise B1.)

Notice that we obtain the same answer, s , in each case. This is because essentially both $b \circ (a \circ t)$ and $(b \circ a) \circ t$ mean ‘do t , then a , then b ’.

In the same way, if F is *any* plane figure, and f , g and h are *any* symmetries in $S(F)$, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

We express this fact by saying that composition of symmetries is *associative*. So our second important property is as follows.

Proposition B2 Associativity property for symmetries

Composition of symmetries is associative; that is, if F is a plane figure, then for all $f, g, h \in S(F)$,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

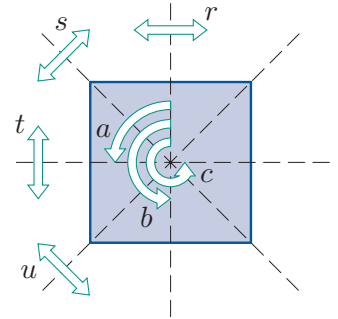


Figure 19 $S(\square)$

For practical purposes, associativity means that we do not need to use brackets when we write a composite of three elements: there is no ambiguity in writing simply $h \circ g \circ f$, without brackets, because it does not matter whether we interpret it as $h \circ (g \circ f)$ or $(h \circ g) \circ f$, as both give the same answer.

In fact, associativity tells us that we can write a composite of *any finite number* of elements without brackets; for example we can write $k \circ h \circ g \circ f$, where f, g, h and k are all symmetries of a figure F , without ambiguity. You will see more explanation of this in Subsection 4.1.

Exercise B4

Check that, in $S(\square)$,

$$a \circ (t \circ a) = (a \circ t) \circ a.$$

(In Worked Exercise B1 we found that $a \circ t = u$ and $t \circ a = s$.)

Existence of an identity

At the beginning of this subsection, it was mentioned that any plane figure has at least one symmetry – the identity symmetry. The existence of an identity is our third important property of a set of symmetries. The identity symmetry e has the property that when it is composed with any symmetry $f \in S(F)$, in either order, the result is simply f .

Proposition B3 Identity property for symmetries

The set $S(F)$ of symmetries of a plane figure F contains a special symmetry e (the **identity symmetry**) such that, for each symmetry f in $S(F)$,

$$f \circ e = f = e \circ f.$$

Existence of inverses

We now consider our fourth and final important property of sets of symmetries of plane figures. This property depends on the fact that a symmetry is a one-to-one and onto function from \mathbb{R}^2 to \mathbb{R}^2 . This is because a symmetry, being an isometry, maps \mathbb{R}^2 *rigidly* onto itself.

Because a symmetry $f \in S(F)$ is a one-to-one and onto function from \mathbb{R}^2 to \mathbb{R}^2 , it has an inverse function $f^{-1} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$. Moreover, since f preserves distances and maps F to itself, so must f^{-1} . In other words, f^{-1} is also a symmetry of F , so $f^{-1} \in S(F)$. You saw in Unit A1 that the composite of f and f^{-1} , in either order, is the identity function; that is, it is the identity symmetry e . These conclusions form our fourth important property, stated below.

Proposition B4 Inverses property for symmetries

Each symmetry f in the set $S(F)$ of symmetries of a plane figure F has an **inverse** symmetry f^{-1} in $S(F)$, such that

$$f \circ f^{-1} = e = f^{-1} \circ f.$$

To illustrate this property, let us look again at $S(\square)$.

Worked Exercise B2

Write down the inverse of each of the elements of $S(\square)$.

(The elements of $S(\square)$, except the identity element e , are shown in Figure 20.)

Solution

The symmetry a is a rotation through $\pi/2$ about the centre, so its inverse is a rotation through $-\pi/2$ (that is, $\pi/2$ clockwise). This is the same symmetry as c , a rotation through $3\pi/2$.

So c is the inverse of a . Similarly, a is the inverse of c .

The symmetry b is a rotation through a half-turn. Composing b with itself returns the square to its original position. So b is its own inverse.

The symmetries r , s , t and u are all reflections. Composing a reflection with itself returns the square to its original position, so each of these symmetries is its own inverse.

Finally, composing the identity symmetry e with itself returns the square to its original position, so e is also its own inverse.

The inverses of the elements of $S(\square)$ are as follows.

Element	e	a	b	c	r	s	t	u
Inverse	e	c	b	a	r	s	t	u

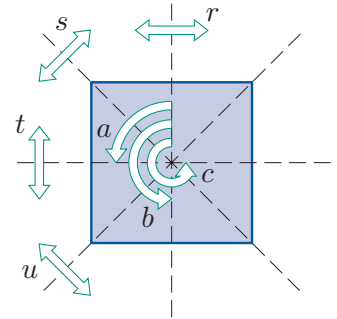


Figure 20 $S(\square)$

If a symmetry of a figure is its own inverse, then we say that it is **self-inverse**. Worked Exercise B2 shows that the elements e , b , r , s , t and u of $S(\square)$ are all self-inverse.

Exercise B5

Draw up a table of inverses for each of the following sets of symmetries.

- (a) $S(\ast)$ (b) $S(\square)$ (c) $S(\triangle)$

We will return to these four important properties of sets of symmetries of plane figures in Section 3.

1.3 Symmetries of the disc

A bounded figure that we have not yet considered is the disc. Figure 21 shows a rotational symmetry and a reflectional symmetry of the disc.



Figure 21 A rotational symmetry and a reflectional symmetry of the disc

Rotation about the centre through any angle is a symmetry of the disc. Likewise, reflection in any line through the centre is a symmetry of the disc. Thus the disc has infinitely many rotational symmetries and infinitely many reflectional symmetries.

We cannot use individual letters to label these infinitely many symmetries, so we denote a rotation about the centre through an angle θ by r_θ , and a reflection in the axis of symmetry making an angle θ with the horizontal axis by q_θ , as shown in Figure 22.



Figure 22 Standard labelling for rotational and reflectional symmetries of the disc

For any integer k , rotations through θ and $\theta + 2k\pi$ produce the same effect as each other, as illustrated in Figure 23(a) for $k = 1$, so we can restrict the angles of rotation to the interval $[0, 2\pi)$. Reflection in the line at an angle θ to the horizontal produces the same effect as reflection in the line at an angle $\theta + \pi$ to the horizontal (in fact, it is the same line), as illustrated in Figure 23(b), so we can restrict the angles for axes of symmetry to the interval $[0, \pi)$.

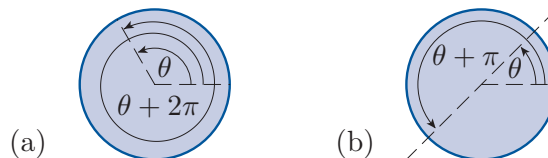


Figure 23 (a) Two angles of rotation that give the same symmetry (b) Two angles that correspond to the same axis of symmetry

So the symmetries of the disc are:

- r_θ : rotation through an angle θ about the centre,
for $\theta \in [0, 2\pi)$;
- q_θ : reflection in the line through the centre at an angle θ to
the horizontal (measured anticlockwise), for $\theta \in [0, \pi)$.

The identity symmetry e is r_0 , the zero rotation. Note that q_0 is reflection in the horizontal axis and is not the identity symmetry.

We denote the set of symmetries of the disc by $S(\odot)$, read as ‘ S disc’:

$$S(\odot) = \{r_\theta : \theta \in [0, 2\pi)\} \cup \{q_\theta : \theta \in [0, \pi)\}.$$

We can compose the symmetries of the disc using diagrams similar to those that we used when composing symmetries of the square. Imagine a paper model of the disc, coloured light blue on one side and a darker blue on the other, with a dot marked at the same place on both sides, as if the dot goes through the paper. We will take the initial position of the disc to be with the light side showing and the dot at the right.

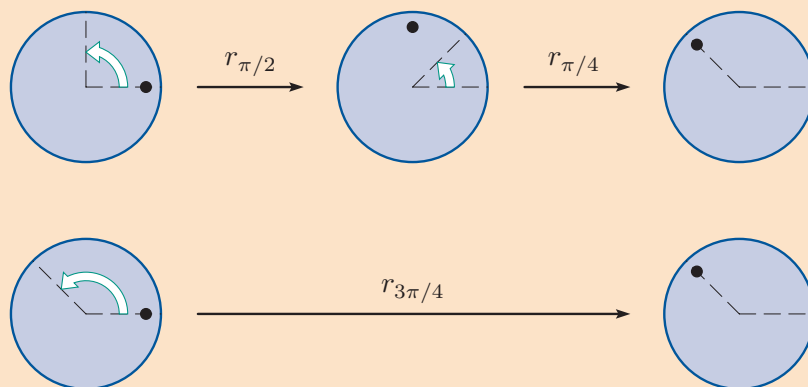
Worked Exercise B3

Find the following composites of symmetries of the disc.

- (a) $r_{\pi/4} \circ r_{\pi/2}$ (b) $q_{\pi/4} \circ q_{\pi/2}$ (c) $q_{\pi/4} \circ r_{\pi/2}$

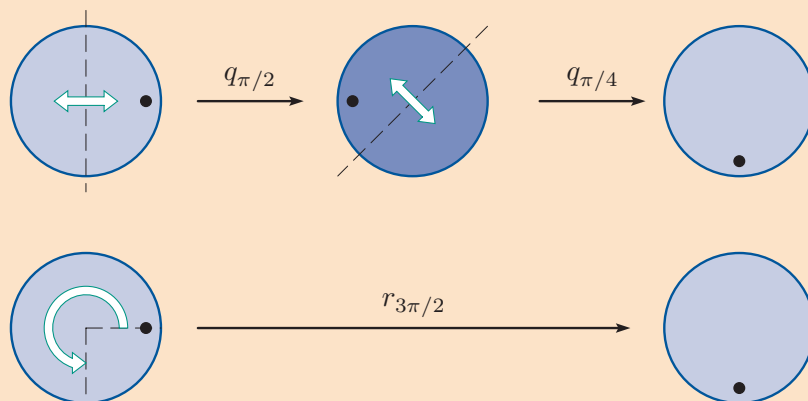
Solution

(a)

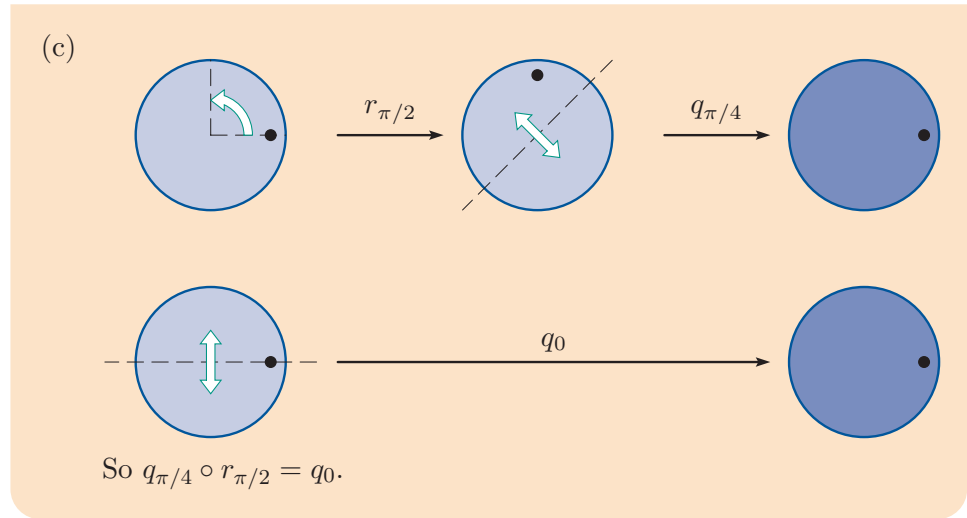


$$\text{So } r_{\pi/4} \circ r_{\pi/2} = r_{3\pi/4}.$$

(b)



$$\text{So } q_{\pi/4} \circ q_{\pi/2} = r_{3\pi/2}.$$



Exercise B6

Find the composite $r_{\pi/4} \circ q_{\pi/2}$.

There are concise formulas for composing any two symmetries of the disc without having to draw diagrams, but we will not need these formulas in this module.

1.4 Direct and indirect symmetries

In most of the sets of symmetries of plane figures that we have considered, the symmetries are of two sorts: those that we can demonstrate with a paper model without turning it over, and those for which we need to take the model out of the plane, turn it over and replace it in the plane. If we use a paper model that is light on one side and dark on the other, and the initial position is with the light side showing, then the symmetries of the former type are those that result in a final position with the light side showing, and the symmetries of the latter type are those that result in a final position with the dark side showing. We make the following definitions.

Definitions

The symmetries of a plane figure F that we can demonstrate with a paper model without lifting it out of the plane to turn it over are called **direct** symmetries. We denote the set of direct symmetries of a figure F by $S^+(F)$.

The remaining symmetries are called **indirect** symmetries: they are the symmetries that cannot be demonstrated with the paper model without lifting it out of the plane, turning it over and then replacing it in the plane.

For a *bounded* plane figure, the direct symmetries are rotations and the indirect symmetries are reflections. For example, the direct symmetries of the square are the rotations e , a , b and c , so

$$S^+(\square) = \{e, a, b, c\}.$$

The indirect symmetries of the square are the reflections r , s , t and u .

In general, consider any plane figure F that has a finite number of symmetries, and think of our usual type of paper model of F , light on one side and dark on the other. Take the starting position to be a position with the light side showing. Let the number of direct symmetries of F be n . In other words, there are n different ways to pick up the paper model of the figure and place it back down to occupy the same region, with the light side showing. If the figure F has *no* indirect symmetries, then these n direct symmetries are the *only* symmetries of F .

Now suppose that F has at least one indirect symmetry. In other words, it is possible to pick up the paper model of F , turn it over and place it back down to occupy the same region, but with the dark side showing. Once you have done that, there must be n different ways in which you can pick up the paper model again and place it back down to occupy the same region, with the dark side still showing. In other words, F has n indirect symmetries, and if you choose any one of them, then you can obtain all n of them by composing the one that you chose with each of the n direct symmetries in turn.

Figure 24 illustrates this for the square. It shows that each of the four reflections of the square can be obtained by turning the model over and then rotating it.

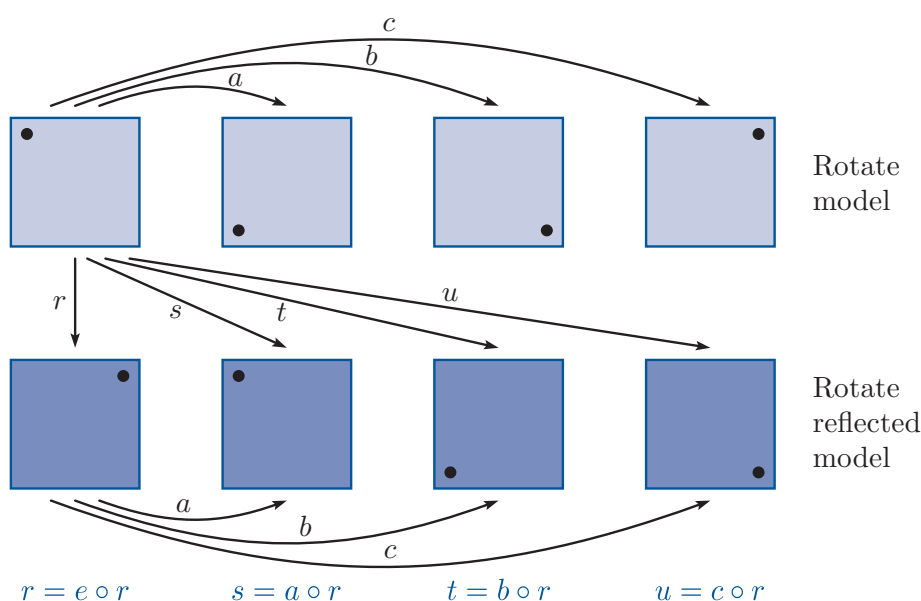


Figure 24 The direct and indirect symmetries of the square

So we have the following useful result.

Theorem B5

If a plane figure has a finite number of symmetries, then either

- all the symmetries are direct, or
- half of the symmetries are direct and half are indirect.

For example, the 4-windmill has only direct symmetries, whereas for the square half of the symmetries are direct and half are indirect.

Exercise B7

- (a) List the elements of the set of direct symmetries of the equilateral triangle, and draw a diagram (similar to Figure 24) to show how the indirect symmetries of the equilateral triangle can be obtained from the direct symmetries by using just one indirect symmetry.
- Use the standard labelling for the elements of $S(\triangle)$, shown in Figure 25, and take the initial position of the triangle to be with the light side showing and the dot in the top corner, as shown below.
- (b) Repeat part (a) for the rectangle. Use the standard labelling for the elements of $S(\square)$, shown in Figure 26, and take the initial position to be as shown below.

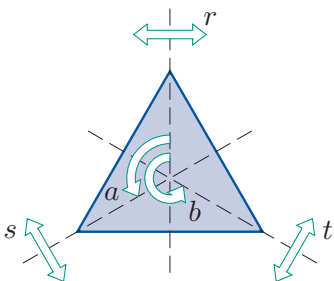


Figure 25 $S(\triangle)$

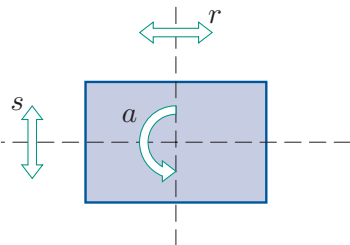


Figure 26 $S(\square)$

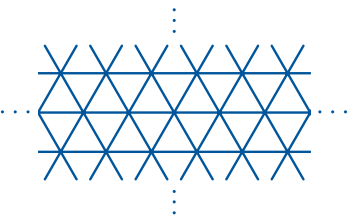


Figure 27 An infinite triangular grid

In Subsection 1.2 you saw some results about composites of rotations and reflections. These can be generalised to corresponding results about direct and indirect symmetries, as follows:

direct \circ direct = direct,	\circ	direct	indirect
direct \circ indirect = indirect,	direct	direct	indirect
indirect \circ direct = indirect,	indirect	indirect	direct
indirect \circ indirect = direct.			

Notice also that the inverse of a direct symmetry is a direct symmetry, and the inverse of an indirect symmetry is an indirect symmetry. This is because for any symmetry f the composite $f \circ f^{-1}$ is equal to the direct symmetry e , so f and f^{-1} are either both direct or both indirect, by the results about composites above.

You have seen in this section that for a *bounded* plane figure the direct symmetries are rotations, and the indirect symmetries are reflections. For

an *unbounded* plane figure, such as the infinite triangular grid in Figure 27, the direct symmetries are either rotations or translations, and the indirect symmetries are either reflections or glide-reflections. We will not need to consider translations and glide-reflections further in the group theory books of this module, as we will generally be working with bounded figures.

2 Representing symmetries

So far we have represented symmetries of plane figures by letters, and used diagrams or models to work out composites. This method is illuminating but time-consuming. In this section you will learn a notation for symmetries that allows us to compose them easily, though at the expense of geometric intuition.

2.1 Two-line symbols

To introduce this new notation for symmetries, let us again consider the symmetries of the square. In Figure 28 the locations of the vertices of the square have been labelled with the numbers 1, 2, 3 and 4. We consider these numbers to be fixed to the background plane. So the number 1 is always at the top left-hand corner of the square. It does not label the vertex of the square, and so it does not move when we apply a symmetry to the square.

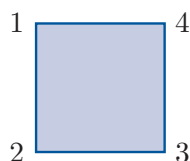


Figure 28 The square with its vertex locations labelled

Here is how we use these numbers to record the effect of a symmetry. Consider, for example, the symmetry a (rotation through $\pi/2$ about the centre), whose effect is shown in Figure 29.

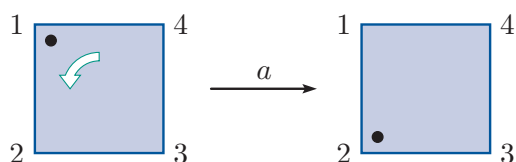


Figure 29 The effect of the symmetry a

This symmetry maps the vertices as follows.

	Shorthand
vertex at location 1 to location 2	$1 \mapsto 2$
vertex at location 2 to location 3	$2 \mapsto 3$
vertex at location 3 to location 4	$3 \mapsto 4$
vertex at location 4 to location 1	$4 \mapsto 1$

We can think of a as a function mapping the set $\{1, 2, 3, 4\}$ to itself:

$$a : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 1 \end{cases} \quad \text{which we might write as} \quad a : \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}.$$

Our new notation for a is based on the version on the right above, with the arrows omitted and the numbers enclosed in brackets. We write

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Remember that, strictly, the symmetries of the square do not act on the numbers 1, 2, 3, 4. In our new notation we are using these numbers as shorthand for ‘the vertex of the square at location 1’, ‘the vertex of the square at location 2’, and so on.

As another example, consider the symmetry r of the square (reflection in the vertical axis), whose effect is shown in Figure 30.

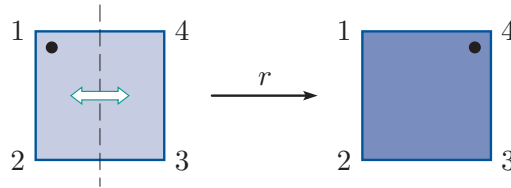


Figure 30 The effect of the symmetry r

This symmetry

interchanges the vertices at locations 1 and 4,

interchanges the vertices at locations 2 and 3.

So, in our new notation, we write

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

The identity symmetry e leaves all the vertices at their original locations, so we write

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

We refer to this new notation for a symmetry of a plane figure as the **two-line symbol** for the symmetry. To specify a symmetry in this form, we must first provide a picture of the figure with labelled locations.

Worked Exercise B4

For the square with vertex locations labelled as shown in Figure 28 (also shown in Figure 31 for convenience), describe geometrically the symmetry represented by the two-line symbol

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Identify it as one of the symmetries a, b, c, r, s, t, u of the square (shown in Figure 31).

Solution

This two-line symbol represents a symmetry that
interchanges the vertices at locations 1 and 2,
interchanges the vertices at locations 3 and 4.



The two-line symbol represents reflection in the horizontal axis. That is, it is the symmetry t .

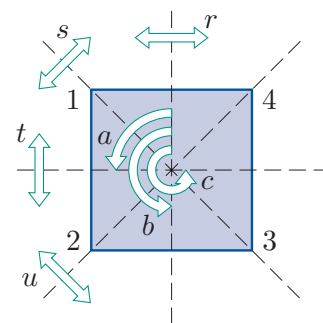


Figure 31 $S(\square)$

Exercise B8

Find the two-line symbols representing the symmetries of the square that we have not yet considered, namely b, c, s and u , using the labelling of locations given in Figure 28 (also shown in Figure 31).

Exercise B9

Find the two-line symbol representing each of the four symmetries of the labelled rectangle in Figure 32. (Note that the locations of the vertices are labelled differently from those of the labelled square in Figure 31.)

The two-line symbols that represent the symmetries of a plane figure depend on the choice of labels for locations. For example, you have seen that reflection in the vertical axis is represented by different two-line symbols for the labelled square in Figure 31 and for the labelled rectangle in Figure 32, because we have used different systems for labelling the locations of the vertices (anticlockwise around the square, but across the top and bottom of the rectangle).

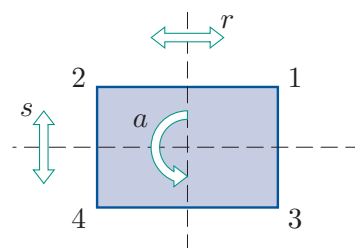


Figure 32 $S(\square)$

Usually, we try to use an anticlockwise labelling of the locations of the vertices, starting at the top left, as illustrated for the square in Figure 33.

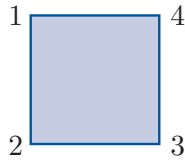


Figure 33 Our usual labelling for the vertex locations of the square

The box below gives a formal definition of a two-line symbol representing a symmetry of a polygon.

Definitions

Let f be a symmetry of a polygon F that has vertices at locations labelled $1, 2, 3, \dots, n$. The **two-line symbol** representing f is

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}.$$

where $f(1), f(2), f(3), \dots, f(n)$ are the labels of the locations to which f moves the vertices originally at the locations labelled $1, 2, 3, \dots, n$, respectively.

We say that f is written in **two-line notation**.

The order of the columns in a two-line symbol is not important, though we usually use the natural order to aid recognition. For example, we usually write the two-line symbol

$$\begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \text{as} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Note that not all possible two-line symbols represent symmetries of a particular figure. For example, with our usual choice of labels for the vertex locations of the square, as shown in Figure 33, the two-line symbol

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

is not a symmetry of the square, because there is no symmetry of the square that interchanges the vertices at locations 2 and 3, and leaves the vertices at locations 1 and 4 fixed.

With our usual location labels, as shown in Figure 34, the two-line symbols for the eight symmetries of the square are as follows.

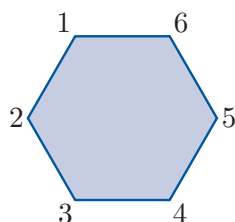
Rotations	Reflections
$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$	$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$
$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$	$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$
$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$	$t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
$c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$	$u = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

Exercise B10

Using the labelling in Figure 35 for the locations of the vertices, write down the two-line symbol for each of the symmetries of the equilateral triangle.

Exercise B11

The following two-line symbols represent symmetries of the labelled hexagon shown below. Describe each symmetry geometrically.



(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}$

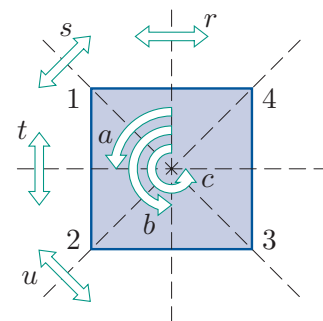


Figure 34 $S(\square)$

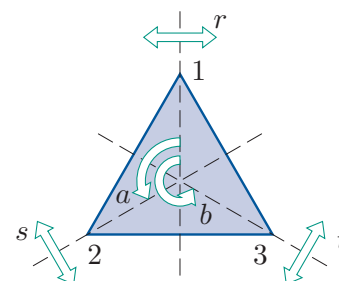


Figure 35 $S(\triangle)$

2.2 Composing and inverting symmetries in two-line notation

One advantage of the two-line notation for symmetries is that it makes it easy to find composites and inverses, without drawing diagrams.

Let us start by looking at composites. In the next worked exercise, we use two-line notation to find the composite of two symmetries of the square.

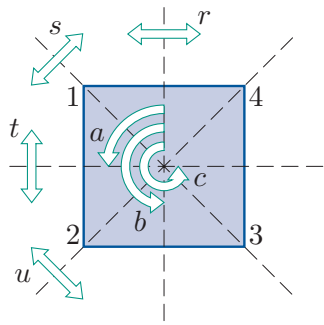


Figure 36 $S(\square)$

The symmetries and standard vertex location labels for the square are repeated in Figure 36 for convenience.

Worked Exercise B5

Use two-line symbols to find the composite $r \circ a$ in $S(\square)$.

Solution

Write down the two-line symbols for r and a (which we found in Subsection 2.1), along with the top row of the two-line symbol for $r \circ a$. Remember that $r \circ a$ means we perform a first, then r .

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}.$$

Find each of the entries in the bottom row of $r \circ a$ in turn. First, a sends 1 to 2 and r sends 2 to 3, so $r \circ a$ sends 1 to 3.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & & & \end{pmatrix}.$$

Next, a sends 2 to 3 and r sends 3 to 2, so the composite sends 2 to 2.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & & \end{pmatrix}.$$

Find the final two entries in the same way: a sends 3 to 4 and r sends 4 to 1, so $r \circ a$ sends 3 to 1; and a sends 4 to 1 and r sends 1 to 4, so $r \circ a$ sends 4 to 4.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

We see that $r \circ a$ interchanges the vertices at locations 1 and 3, and keeps the vertices at 2 and 4 where they are. Thus $r \circ a$ is the reflection u .

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = u.$$

Remember that the order of composition of symmetries is important. For example,

$$a \circ r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = s,$$

so

$$r \circ a \neq a \circ r.$$

Exercise B12

Using the two-line symbols for the symmetries of the equilateral triangle (you were asked to find these in Exercise B10), find the following composites:

$$a \circ a, \quad b \circ s, \quad s \circ b, \quad t \circ s.$$

(The symmetries and standard vertex location labels are shown in Figure 37 for convenience.)

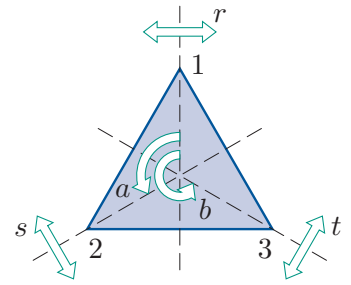


Figure 37 $S(\triangle)$

Now let us look at finding the inverses of symmetries in two-line notation. You saw in Section 1 that every symmetry has an inverse, which ‘undoes’ the effect of the symmetry.

The worked exercise below demonstrates the method for finding the inverse of a symmetry given as a two-line symbol.

Worked Exercise B6

Find the inverse of the symmetry a in $S(\square)$.

Solution

Find the two-line symbol for a .

We have

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Remember that the inverse a^{-1} ‘undoes’ the effect of a . So, since a sends 1 to 2, a^{-1} must send 2 to 1; since a sends 2 to 3, a^{-1} must send 3 to 2; and so on. Thus to find a^{-1} , we just have to turn the two-line symbol for a ‘upside down’.

So

$$a^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Usually, we then rearrange the columns into the natural order, to make the inverse easier to recognise.

$$\begin{aligned} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\ &= c. \end{aligned}$$

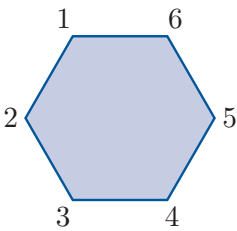


Figure 38 The hexagon, with vertex locations labelled

Exercise B13

Find the inverse of each of the following symmetries of the labelled regular hexagon shown in Figure 38. Give your answers as two-line symbols.

- (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$

2.3 Cayley tables

A useful way to record composites of symmetries is to use a **Cayley table**. To construct a Cayley table for the symmetries of a figure F , we list the elements of $S(F)$ across the top and down the left-hand side of a square array, as illustrated below.

	e	f	g	\cdots	x	y	z
e							
f							
g							
\vdots							
x							
y							
z							

The order in which we list the elements is not important, but it is important to use the *same order* across the top and down the side. Normally we put the identity symmetry e first, as shown above.

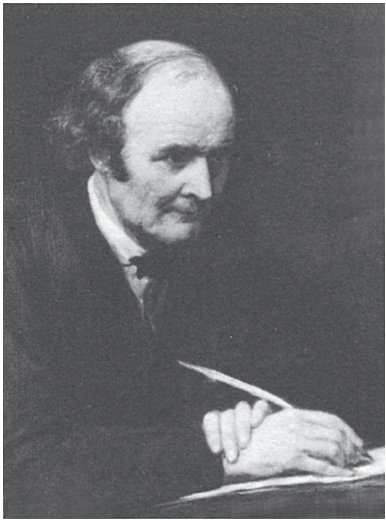
This square array enables us to display every possible composite of pairs of elements in $S(F)$. However, this is practicable only if $S(F)$ is a small set, and it is not possible for $S(\bigcirc)$, which is infinite!

For any two elements x and y of $S(F)$, we record the composite $x \circ y$ in the cell in the row labelled x and the column labelled y .

	\cdots	y	\cdots
\vdots		\vdots	
x	\cdots	$x \circ y$	\cdots
\vdots		\vdots	

Note that x is on the left both in the composite and in the border of the table. Of course, the composite $x \circ y$ is the result of performing first the symmetry y and then the symmetry x .

Arthur Cayley (1821–1895) was the leading British algebraist of the nineteenth century. He helped to lay the groundwork for the abstract theory of groups, and he developed the algebra of matrices and determinants. Prior to his appointment in 1863 as the first professor of pure mathematics at the University of Cambridge, he spent fourteen years as a lawyer during which time he produced over three hundred mathematical papers.



Arthur Cayley

We have found many composites of elements of $S(\square)$ already; for example, $a \circ t = u$, $t \circ a = s$ and $r \circ a = u$. A complete Cayley table for $S(\square)$ is given below. The elements of $S(\square)$ are shown in Figure 39.

\circ	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

Exercise B14

A partially-completed Cayley table for $S(\triangle)$ is shown below. (You were asked to find some of the composites here in Exercise B12, and some others in Exercise B3(c).)

Complete the table, using the two-line symbols from Exercise B10 to work out the required composites. The elements of $S(\triangle)$ are shown in Figure 40.

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e		s	t	
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r		a	b	

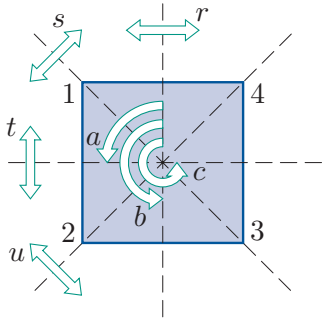


Figure 39 $S(\square)$

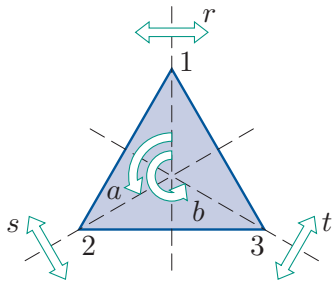


Figure 40 $S(\triangle)$

Exercise B15

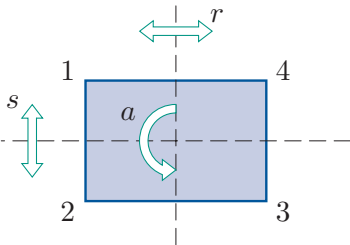


Figure 41 $S(\square)$

Complete the following Cayley table for $S(\square)$. The labelling of the symmetries is as shown in Figure 41.

\circ	e	a	r	s
e	e	a	r	s
a	a		s	
r	r	s	e	a
s	s		a	

You may have noticed a ‘blocking’ effect in the Cayley table for $S(\square)$ above, as highlighted in Figure 42(a), and a similar effect in the Cayley table for $S(\triangle)$ found in Exercise B14. This effect occurs because we have chosen to list all the direct symmetries first in the borders of the table, followed by the indirect symmetries, and, as you saw earlier, a composite of any two direct symmetries or any two indirect symmetries is always a direct symmetry, and a composite of a direct symmetry and an indirect symmetry is always an indirect symmetry. This gives the blocking shown in Figure 42(b).

\circ	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

(a)

\circ	direct	indirect
direct	direct	indirect
indirect	indirect	direct

(b)

Figure 42 ‘Blocking’ into direct and indirect symmetries

A similar blocking effect occurs in the Cayley table for the set of symmetries of any plane figure that has indirect symmetries, when we list all the direct symmetries first in the borders of the table.

3 Definition of a group

You are now ready to learn what is meant by a *group*.

3.1 The group axioms

In Subsection 1.2 you saw that if F is a plane figure, then any two symmetries in the set $S(F)$ of symmetries of F can be composed, and the following four properties hold.

- **Closure** The composite of any two symmetries in $S(F)$ is a symmetry in $S(F)$.
- **Associativity** Composition of symmetries is associative.
- **Identity** The set $S(F)$ contains an identity symmetry.
- **Inverses** Each symmetry f in $S(F)$ has an inverse symmetry.

There are many other circumstances in which we have some set, with a means of combining any two elements of the set, in which four properties analogous to those above hold. For example, consider the set \mathbb{R} of real numbers, with addition as the means of combining any two elements. As you know from Unit A2 *Number systems*, the following four properties hold; compare them to the properties above.

- **Closure** (A1) The sum of any two numbers in \mathbb{R} is a number in \mathbb{R} .
- **Associativity** (A2) Addition of numbers in \mathbb{R} is associative (that is, $(x + y) + z = x + (y + z)$ for all $x, y, z \in \mathbb{R}$).
- **Identity** (A3) The set \mathbb{R} contains an identity element (namely 0, since adding 0 to any real number leaves the number unchanged).
- **Inverses** (A4) Every number in \mathbb{R} has an inverse number (the inverse of x is $-x$, because adding x and $-x$ gives the identity element 0).

A means of combining any two elements of a set is called a **binary operation** on the set. For example, function composition is a binary operation on the set of symmetries of a figure, and addition is a binary operation on the set \mathbb{R} . Similarly, multiplication is a binary operation on the set \mathbb{R} , and addition modulo n and multiplication modulo n are binary operations on the set $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$, for any integer $n \geq 2$.

When we have a set, together with a binary operation on the set, such that four properties analogous to those above hold, we say that the set and the binary operation together form a mathematical structure known as a *group*. So the set of symmetries of a figure with the operation of function composition forms a group, as does the set \mathbb{R} with the operation of addition.

Here is the formal definition of a group. In this definition, G represents a set of any kind of objects, and \circ (which is read, as usual, as ‘circle’) represents any binary operation defined on G (it does not necessarily represent function composition). The set G may be either finite or infinite.

Definition

Let G be a set and let \circ be a binary operation defined on G . Then (G, \circ) is a **group** if the following four axioms hold.

G1 Closure For all g, h in G ,

$$g \circ h \in G.$$

G2 Associativity For all g, h, k in G ,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

G3 Identity There is an element e in G such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for \circ on G .)

G4 Inverses For each element g in G , there is an element h in G such that

$$g \circ h = e = h \circ g.$$

(The element h is an **inverse element** of g with respect to \circ .)

We refer to axioms G1–G4 as the **group axioms**. In mathematics, an **axiom** is a mathematical statement that is used as a starting point from which other mathematical statements are deduced.

We often refer to an identity element simply as an **identity**, and to an inverse element of an element g simply as an **inverse** of g . An alternative way to say that (G, \circ) is a group is to say that G is a group **under** \circ .



Évariste Galois

The word *group* was introduced by the French mathematician Évariste Galois (1811–1832), as part of a theory to classify the polynomial equations whose solutions can be expressed by a formula involving *radicals* (n th roots). However, what Galois meant by a group was somewhat different to the modern definition of the term. His memoir on this topic, which was written in 1830, lay unpublished until 1846, several years after his untimely death from wounds received in a duel.

Notice that the binary operation \circ of a group need *not* have the property that

$$g \circ h = h \circ g \quad \text{for all } g, h \text{ in } G.$$

That is, the binary operation does not have to be **commutative**. A group that has this additional property is given a special name.

Definitions

A group (G, \circ) that has the additional property that

$$g \circ h = h \circ g \quad \text{for all } g, h \text{ in } G$$

is an **abelian** (or **commutative**) group.

A group that is not abelian is **non-abelian**.

For example, the set of real numbers, with addition, is an abelian group, because addition of real numbers is commutative. On the other hand, the set of symmetries of the square, with function composition, is a non-abelian group, since composing symmetries of the square in different orders can give different results, as you saw in Subsection 1.2.

Abelian groups are named after the Norwegian mathematician Niels Henrik Abel (1802–1829), who in 1824 showed that no formula involving radicals exists for the solutions of a general polynomial equation of degree 5. Formulas for the solutions of general polynomial equations of degrees 3 and 4 had been found in the 16th century, although they were written without the benefit of modern notation.

Since Abel initially had to publish his result at his own expense, he compressed the proof in order to save money, and this made it very hard to understand. It was only later, after he had the opportunity to rewrite an elaborated version for publication in a German journal, that his work became widely known.



Niels Henrik Abel

Here are some more definitions that are useful when we discuss groups.

Definitions

- If the set G of a group (G, \circ) is a finite set, then we say that (G, \circ) is a **finite** group. If G has exactly n elements, then we say that (G, \circ) is a group of **order** n , and we write $|G| = n$.
- If the set G of a group (G, \circ) is an infinite set, then we say that (G, \circ) is an **infinite** group and that it has **infinite order**.

For example, the set $S(\square)$ of symmetries of the square, with function composition, is a finite group and has order 8. We write $|S(\square)| = 8$. The set of real numbers, with addition, is an infinite group.

As you saw in Unit A2 *Number systems*, an identity element for a binary operation on a set is sometimes called an **additive identity** if the binary operation is addition, and a **multiplicative identity** if the binary operation is multiplication. Similarly, an inverse of a particular element is sometimes called an **additive inverse** if the binary operation is addition, and a **multiplicative inverse** if the binary operation is multiplication.

In Unit A2 you saw that a *field* is a set with two operations, $+$ and \times , such that twelve properties hold. These twelve properties are called the *field axioms*, though we did not use that term in Unit A2. A field can be defined more concisely in terms of groups, as follows. If F is a set, and $+$ and \times are binary operations defined on F , then we say that $(F, +, \times)$ is a **field** if it has the following three properties.

- $(F, +)$ is an abelian group.
- $(F - \{0\}, \times)$ is an abelian group (where 0 is the identity element for $+$ on F).
- The distributive law $x \times (y + z) = (x \times y) + (x \times z)$ holds for all $x, y, z \in F$.

3.2 Checking the group axioms

To show that a given set and binary operation form a group, we need to check that they satisfy the four group axioms.

The worked exercise below demonstrates how to show formally that the set \mathbb{R} of real numbers, with addition, forms a group.



Worked Exercise B7

Show that $(\mathbb{R}, +)$ is a group.

Solution

We show that the four group axioms hold.

G1 Closure


 We have to check that if we add any two elements of \mathbb{R} , then we always get another element of \mathbb{R} . We can use x and y , say, to denote general elements of \mathbb{R} . 

For all $x, y \in \mathbb{R}$,

$$x + y \in \mathbb{R}.$$



So \mathbb{R} is closed under addition.

G2 Associativity

 We already know that addition of numbers is an associative operation. 

Addition of real numbers is associative.

G3 Identity



 We have to check that the set \mathbb{R} contains a special element such that, when this element is added to any other element, in either order, the result is simply that other element. 

We have $0 \in \mathbb{R}$, and for all $x \in \mathbb{R}$,

$$x + 0 = x = 0 + x.$$

So 0 is an identity element for addition on \mathbb{R} .

G4 Inverses

 We have to check that for each element x in \mathbb{R} , there is an element in \mathbb{R} such that, when this element is added to x , in either order, the result is the identity element 0. 

For each $x \in \mathbb{R}$, we have $-x \in \mathbb{R}$, and

$$x + (-x) = 0 = (-x) + x,$$

so $-x$ is an inverse of x .

Thus each element of \mathbb{R} has an inverse element in \mathbb{R} with respect to addition.

Hence $(\mathbb{R}, +)$ satisfies the four group axioms, and so is a group.

There are several things that it is useful to observe about Worked Exercise B7.

First, notice that when you check axioms G3 (identity) and G4 (inverses), you have to check *both possible orders* of combining two elements. For example, when we checked axiom G3 in Worked Exercise B7, we checked not only that $x + 0 = x$, but also that $0 + x = x$. Similarly, when we checked axiom G4, we checked not only that $x + (-x) = 0$, but also that $(-x) + x = 0$. This checking was straightforward in Worked Exercise B7, because the binary operation was addition, and order does not matter when you add two numbers. However, for some binary operations the checking can involve more work.

Second, notice that when we checked axiom G3 (identity) in Worked Exercise B7, it was fairly obvious that the identity element had to be 0. In general, if you are dealing with a set of numbers and the binary operation is ordinary addition, then the only possible identity element is 0. (This is because the only possibility for a number e that satisfies the equation $g + e = g$ for all numbers g is $e = 0$.) Similarly, if you are dealing with a set of numbers and the binary operation is ordinary multiplication, then the only possible identity element is 1. For other binary operations, *including modular addition and modular multiplication*, it may be less obvious what the identity element has to be. You just have to try to find a possibility and check that it works.

A similar point applies to axiom G4 (inverses). If you are dealing with a set of numbers and the binary operation is ordinary addition, then the only possible inverse of an element x is $-x$; if you are dealing with a set of numbers and the binary operation is ordinary multiplication, then the only possible inverse of an element x is $1/x$. For other binary operations it may be less obvious what the inverses have to be.

Third, notice that when you check axiom G3 (identity) it is not enough to check that a particular element *is* an identity element. You also have to check that this element *actually lies in the set* that you are considering. Similarly, when you check axiom G4 (inverses), not only do you have to check that each element *has* an inverse, you also have to check that each inverse *lies in the set* that you are considering.

Finally, notice that when you check axiom G2 (associativity), if the binary operation that you are dealing with is one that you already know is associative, such as the operations in the box below, then you can simply state that it is associative, without proof. We did this in Worked Exercise B7. However, if the binary operation is unfamiliar, then you have to provide a proof of associativity.

Standard associative binary operations

- Addition
- Multiplication
- Function composition
- Modular addition
- Modular multiplication

You might find it helpful to refer back to the comments above as you work through the rest of this subsection. Below is another worked exercise that illustrates some of these points. Here the binary operation is multiplication (rather than addition, as in the previous worked exercise). The set is \mathbb{R}^* , that is, the set $\mathbb{R} - \{0\}$ of all the real numbers except 0.



Worked Exercise B8

Show that (\mathbb{R}^*, \times) is a group.

Solution

We show that the four group axioms hold.

G1 Closure

 We have to check that if we multiply any two elements of \mathbb{R}^* , we always get another element of \mathbb{R}^* . To specify that x and y , say, represent *any* elements of \mathbb{R}^* , we can say ‘Let $x, y \in \mathbb{R}^*$.’ 



Let $x, y \in \mathbb{R}^*$. Then, since x and y are real numbers, so is $x \times y$.

Also $x \times y \neq 0$, since $x \neq 0$ and $y \neq 0$. Hence

$$x \times y \in \mathbb{R}^*,$$



so \mathbb{R}^* is closed under multiplication.

G2 Associativity

 We already know that multiplication of numbers is associative. 

Multiplication of real numbers is associative.

G3 Identity



 We have to check that the set \mathbb{R}^* contains a special element such that when this element is multiplied by any other element, in either order, the result is simply that other element. 

We have $1 \in \mathbb{R}^*$, and for all $x \in \mathbb{R}^*$,

$$x \times 1 = x = 1 \times x.$$

So 1 is an identity element for multiplication on \mathbb{R}^* .

G4 Inverses

 We have to check that for each element x in \mathbb{R}^* , there is an element in \mathbb{R}^* such that when this element is multiplied by x , in either order, the result is the identity element 1. 

Let $x \in \mathbb{R}^*$. Then $x \neq 0$, so $1/x$ exists, and lies in \mathbb{R}^* , since $1/x \neq 0$. Also

$$x \times \frac{1}{x} = 1 = \frac{1}{x} \times x.$$

Hence $1/x$ is an inverse of x .

Thus each element of \mathbb{R}^* has an inverse element in \mathbb{R}^* with respect to multiplication.

Hence (\mathbb{R}^*, \times) satisfies the four group axioms, and so is a group.

You can practise applying the four group axioms for yourself in the next exercise. The notation \mathbb{Q}^* in part (b) denotes the set $\mathbb{Q} - \{0\}$ of all the rational numbers except 0.

Exercise B16

Show that each of the following is a group.

- (a) $(\mathbb{Z}, +)$ (b) (\mathbb{Q}^*, \times)

You have seen that to prove that a set G and binary operation \circ form a group, you have to show that all four group axioms hold. It follows that to show that a set and binary operation *do not* form a group, you just need to show that *any one* of the four group axioms fails. Here is an example.

Worked Exercise B9



Show that (\mathbb{R}, \times) is not a group.

Solution

 We check each axiom in turn until we find one that fails. 

We check the four group axioms.

G1 Closure

 If we multiply any two elements of \mathbb{R} , do we always get another element of \mathbb{R} ? 

For all $x, y \in \mathbb{R}$,

$$x \times y \in \mathbb{R}.$$

So \mathbb{R} is closed under multiplication.



 Axiom G1 holds. 

G2 Associativity

Multiplication of real numbers is associative.

 Axiom G2 holds. 

G3 Identity

 Does \mathbb{R} contain a special element such that when this element is multiplied by any other element, in either order, the result is that other element? 

We have $1 \in \mathbb{R}$, and for all $x \in \mathbb{R}$,

$$x \times 1 = x = 1 \times x.$$

So 1 is an identity element for \times on \mathbb{R} (and the only possibility to be such an identity element).

 Axiom G3 holds. 

G4 Inverses

☁ For each element x in \mathbb{R} , is there is an element in \mathbb{R} such that when this element is multiplied by x , in either order, the result is the identity element 1?

No! For nearly every element x in \mathbb{R} , the element $1/x$ has the required property. But there is no element with the required property for 0. ☁

The element 0 is in \mathbb{R} , but it has no inverse with respect to multiplication in \mathbb{R} . This is because there is no element y , say, in \mathbb{R} that has the property that

$$0 \times y = 1.$$

Hence axiom G4 does not hold.

It follows that (\mathbb{R}, \times) is not a group.

In general, to show that a particular set and binary operation do not form a group, you need to show that one of the group axioms fails, by demonstrating that there is a counterexample to the axiom. For instance, in Worked Exercise B9 we pointed out that, for the set \mathbb{R} and binary operation \times , the number 0 is a counterexample to axiom G4 (inverses).

Although in Worked Exercise B9 we checked all the group axioms in turn until we found one that failed, if you can immediately spot an axiom that fails, then you can go straight to that axiom and provide a counterexample, without working through the preceding axioms. The only exception to this is that if you want to show that axiom G4 (inverses) fails, then, since you need an identity element for axiom G4 to make sense, you have to begin by establishing what this identity element must be. That is, you have first to consider axiom G3 (identity) to some extent.

The next worked exercise gives, for each of the four axioms, an example of how we can show that the axiom in question fails.

Worked Exercise B10

- (a) Let D be the set of odd integers. Show that $(D, +)$ is not a group, by showing that axiom G1 (closure) fails.
- (b) Show that $(\mathbb{R}, -)$ is not a group, by showing that axiom G2 (associativity) fails.
- (c) Let E be the set of even integers. Show that (E, \times) is not a group, by showing that axiom G3 (identity) fails.
- (d) Show that (\mathbb{N}, \times) is not a group, by showing that axiom G4 (inverses) fails. (Remember that \mathbb{N} is the set of natural numbers, that is, positive integers.)

Solution

- (a) The numbers 3 and 5 lie in D , but

$$3 + 5 = 8 \notin D.$$

So D is not closed under $+$. That is, axiom G1 fails.

- (b) Consider the numbers 6, 4 and 1 in \mathbb{R} . We have

$$6 - (4 - 1) = 6 - 3 = 3,$$

but

$$(6 - 4) - 1 = 2 - 1 = 1.$$

These expressions are not equal, so this counter-example shows that subtraction is not associative on \mathbb{R} . That is, axiom G2 fails.

- (c) There is no element $e \in E$ such that

$$2 \times e = 2,$$

because $1 \notin E$. So (E, \times) has no identity element. That is, axiom G3 fails.

- (d) The number 1 is the only possible identity element for (\mathbb{N}, \times) . However, $2 \in \mathbb{N}$, and there is no number n , say, in \mathbb{N} such that

$$2 \times n = 1,$$

because $\frac{1}{2} \notin \mathbb{N}$. So the element 2 of \mathbb{N} has no inverse in \mathbb{N} . Hence axiom G4 fails.

Sometimes, as in the next exercise, you may need to determine whether a particular set and binary operation form a group, rather than being told this from the start and asked to prove it. In this sort of situation, it is worth having a quick think to see whether you can spot an axiom that fails. Often when a set and binary operation do not form a group, more than one of the axioms fails. If you cannot immediately spot an axiom

that fails, then usually the best way to proceed is to work through the four axioms systematically, until either you have proved that they all hold, or you have found one that fails.

Exercise B17

For each of the following, either show that the given set and binary operation form a group, or show that they do not.

- (a) (\mathbb{Q}, \times)
- (b) $(\mathbb{R}^+, +)$, where \mathbb{R}^+ is the set of positive real numbers.
- (c) (D, \times) , where D is the set of odd integers.
- (d) $(E, +)$, where E is the set of even integers.
- (e) $(E, -)$, where E is the set of even integers.
- (f) (M, \times) , where M is the set whose elements are all the negative real numbers and the number 1; that is, $M = \{x \in \mathbb{R} : x < 0\} \cup \{1\}$.

Unfamiliar binary operations

In all the examples that you have seen so far, the binary operation has been a familiar one, such as addition, multiplication or function composition. In the next worked exercise, the binary operation is unfamiliar.

Worked Exercise B11

Determine whether (\mathbb{R}, \circ) is a group, where \circ is defined by

$$x \circ y = x + y + xy.$$

Solution

We check the four group axioms.

G1 Closure

For all $x, y \in \mathbb{R}$,

$$x \circ y = x + y + xy \in \mathbb{R},$$

since sums and products of real numbers are real numbers. So \mathbb{R} is closed under \circ .

G2 Associativity

For each $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} x \circ (y \circ z) &= x \circ (y + z + yz) \\ &= x + (y + z + yz) + x(y + z + yz) \\ &= x + y + z + yz + xy + xz + xyz \\ &= x + y + z + xy + xz + yz + xyz \end{aligned}$$

and

$$\begin{aligned}
 (x \circ y) \circ z &= (x + y + xy) \circ z \\
 &= (x + y + xy) + z + (x + y + xy)z \\
 &= x + y + xy + z + xz + yz + xyz \\
 &= x + y + z + xy + xz + yz + xyz.
 \end{aligned}$$

The two expressions obtained are the same, so \circ is associative on \mathbb{R} .

G3 Identity

 Try to find a likely candidate to be an identity element. 

We need an element $e \in \mathbb{R}$ such that, for all $x \in \mathbb{R}$,

$$x \circ e = x = e \circ x.$$


The left-hand equation $x \circ e = x$ gives

$$x + e + xe = x,$$

which simplifies to

$$e(1 + x) = 0.$$

Since we need this equation to be true for all $x \in \mathbb{R}$, the only possibility for an identity element is $e = 0$.

 Now check to see whether 0 actually is an identity element. 

Now $0 \in \mathbb{R}$, and for all $x \in \mathbb{R}$,


$$x \circ 0 = x + 0 + x0 = x,$$

and

$$0 \circ x = 0 + x + 0x = x,$$

as required. So 0 is an identity element for \circ on \mathbb{R} .

G4 Inverses

 Try to find a likely candidate to be an inverse of a general element x . 

For each $x \in \mathbb{R}$, we need an element y , say, in \mathbb{R} such that

$$x \circ y = 0 = y \circ x.$$

The left-hand equation $x \circ y = 0$ gives

$$x + y + xy = 0.$$

 Try to solve this equation for y . 



This equation can be rearranged as

$$y(1 + x) = -x,$$

so, for $x \neq -1$,

$$y = -\frac{x}{1+x},$$

and this element is in \mathbb{R} .

 So it looks like every element x in \mathbb{R} except possibly -1 has an inverse, given by $-x/(1+x)$. But what about -1 : does it have an inverse? 

If the element -1 has an inverse y , then

$$(-1) \circ y = 0 = y \circ (-1).$$

The left-hand equation $(-1) \circ y = 0$ gives

$$-1 + y - y = 0,$$

which simplifies to

$$-1 = 0.$$

This conclusion is false, so -1 has no inverse.

Hence axiom G4 fails, and therefore (\mathbb{R}, \circ) is not a group.

In the worked exercise above, you saw that the set \mathbb{R} is not a group under the binary operation \circ given by $x \circ y = x + y + xy$, because the element -1 has no inverse and so axiom G4 fails. In fact, if you remove the element -1 from \mathbb{R} then you *do* obtain a group under this binary operation. There is a ‘challenging’ exercise in the additional exercises booklet for this unit that asks you to prove this.

You can practise working with unfamiliar binary operations in the exercises below.

Exercise B18

Show that (\mathbb{R}, \circ) , where \circ is defined by

$$x \circ y = x - y - 1,$$

is not a group, by showing that group axiom G3 (identity) fails.

Exercise B19

Determine whether each of the following binary operations \circ defined on \mathbb{R} is associative.

(a) $x \circ y = x + y - xy$ (b) $x \circ y = x - y + xy$

Exercise B20

Show that (\mathbb{Q}^+, \circ) is a group, where \mathbb{Q}^+ is the set of positive rational numbers and \circ is defined by $a \circ b = \frac{1}{2}ab$.

3.3 Checking the group axioms for small finite sets

In the previous subsection you saw how to check the group axioms for a variety of sets and binary operations. In all the examples, the set was an infinite set. In this subsection we concentrate on how to check the group axioms when the set is a small finite set.

Most of the examples of small finite sets and binary operations that we will consider in this subsection come from modular arithmetic, which you met in Unit A2. Remember that for any natural number n we have

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\},$$

and the operations $+_n$ and \times_n on \mathbb{Z}_n are defined by

$$a +_n b = \text{the remainder of } a + b \text{ on division by } n,$$

$$a \times_n b = \text{the remainder of } a \times b \text{ on division by } n.$$

For example, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, and we have

$$2 +_4 3 = 1,$$

$$2 \times_4 3 = 2.$$

If we have a small finite set with a binary operation (where the set and binary operation come from modular arithmetic or from anywhere else), then we can construct a Cayley table for them, in the same way as we did for sets of symmetries earlier. As you will see in this subsection, we can use this table to help us check some of the group axioms.

To construct a Cayley table for a small finite set G and binary operation \circ , we use the same approach as for a set of symmetries. We list the elements of G across the top and down the side of a square array, keeping the order of the elements the same across the top and down the side. If we can immediately spot an identity element, then usually we put it first in the list, but this is not essential.

For any two elements x and y of G , we enter the composite $x \circ y$ in the cell in the row labelled x and the column labelled y , as shown below. So x is on the left both in the composite and in the row labels down the left of the table.

\circ	\cdots	y	\cdots
\vdots		\vdots	
x	\cdots	$x \circ y$	\cdots
\vdots		\vdots	

We refer to the lists of elements along the top and down the side of a Cayley table as the **borders** of the table, and we refer to the rest of the table as its **body**. When we mention a row or column of the table, we mean a row or column of the body of the table. The diagonal of the table that goes from the top left to the bottom right, as shown in Figure 43, is called the **main diagonal** (also known as the **leading diagonal**). It contains the results of composing each element with itself.

A Cayley table will help you check group axioms G1 (closure), G3 (identity) and G4 (inverses). However, group axiom G2 (associativity) is time-consuming to check from a Cayley table, so it is best to check it using a known property of the binary operation, if possible.

The next worked exercise demonstrates how to use a Cayley table to check the group axioms for a small finite set. Immediately after the worked exercise there are two propositions whose proofs clarify why the methods used to check axioms G3 (identity) and G4 (inverses) actually do check these axioms.

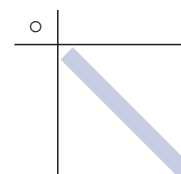


Figure 43 The main diagonal of a Cayley table

Worked Exercise B12

By using a Cayley table, determine whether $(\mathbb{Z}_4, +_4)$ is a group.

Solution

🧠 Construct a Cayley table for $(\mathbb{Z}_4, +_4)$. 🧠

A Cayley table for $(\mathbb{Z}_4, +_4)$ is as follows.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

We now check the group axioms.

G1 Closure

☁ Check that every element in the body of the table belongs to the set that we are considering. ☁

Every element in the body of the table is in \mathbb{Z}_4 , so \mathbb{Z}_4 is closed under $+_4$.

G2 Associativity

☁ Associativity is time-consuming to check from the table, but we already know that the binary operation here is associative. ☁

Modular addition is associative.

G3 Identity

☁ Check that there is an element such that the row labelled by that element and the column labelled by that element repeat the table borders. If there is such an element, then it is an identity element. ☁

The row and column labelled 0 repeat the table borders, so 0 is an identity element for $+_4$ on \mathbb{Z}_4 .

G4 Inverses

☁ To find inverses, look for occurrences of the identity element in the body of the table.

- If it appears on the main diagonal, then the corresponding element in the table borders is self-inverse (the inverse of itself).
- If it appears off the main diagonal, but symmetrically with respect to the main diagonal, then the two corresponding elements in the table borders are inverses of each other.

In the case here, the identity element is 0 and its occurrences are as shown below.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The identity element 0 appears on the main diagonal in the row and column labelled 0. So 0 is self-inverse.

The identity element 0 also appears on the main diagonal in the row and column labelled 2. So 2 is self-inverse.

Finally, the identity element 0 appears symmetrically in the row labelled 1 and column labelled 3, and in the row labelled 3 and column labelled 1. So 1 and 3 are inverses of each other.

So each element has an inverse in \mathbb{Z}_4 with respect to $+_4$.

Hence $(\mathbb{Z}_4, +_4)$ satisfies the four group axioms, and so is a group.

The proposition below justifies the method we used in Worked Exercise B12 for checking axiom G3 (identity).

Proposition B6 Checking a Cayley table for an identity

Let G be a finite set and let \circ be a binary operation on G . Then the element e of G is an identity element for \circ on G if and only if the row and column labelled e both repeat the table borders.

Proof In the Cayley table for (G, \circ) , the row labelled e contains all the composites of the form $e \circ g$, for $g \in G$, and the column labelled e contains all the composites of the form $g \circ e$, for $g \in G$.

So saying that the row labelled e repeats the top border is the same as saying that $e \circ g = g$ for all $g \in G$, and saying that the column labelled e repeats the side border is the same as saying that $g \circ e = g$ for all $g \in G$. (This is illustrated in Figure 44.)

In summary, saying that the row and column labelled e repeat the table borders is equivalent to saying that $g \circ e = g = e \circ g$ for all $g \in G$. That is, it is equivalent to saying that e is an identity element for G . ■

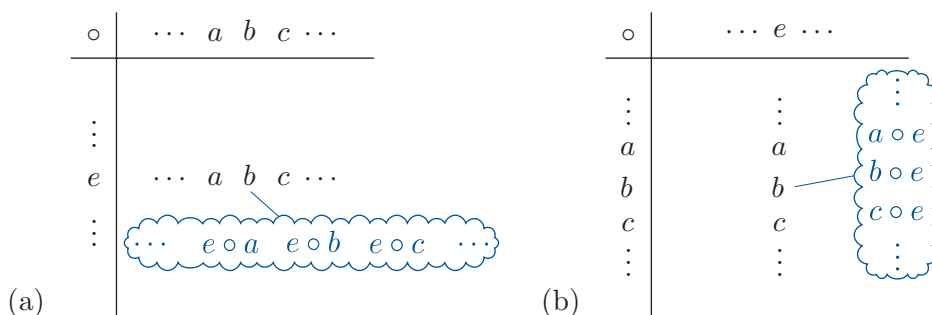


Figure 44 A row and column that repeat the table borders

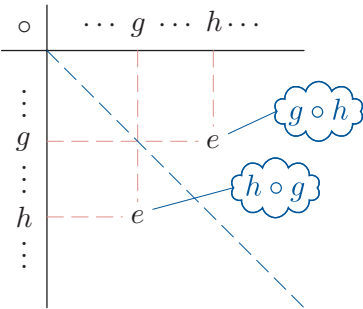


Figure 45 A Cayley table in which $g \circ h = e = h \circ g$

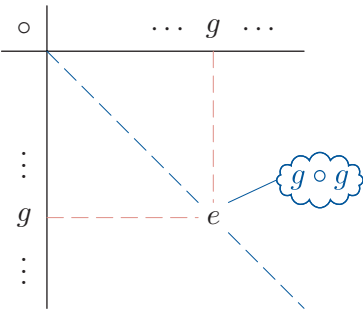


Figure 46 A Cayley table in which $g \circ g = e$

The next proposition justifies the method we used for checking axiom G4 (inverses) in Worked Exercise B12.

Proposition B7 Checking a Cayley table for inverses

Let G be a finite set, let \circ be a binary operation on G and let e be an identity element for \circ on G . Then the element h of G is an inverse of the element g of G if and only if e appears in the position that is in the row labelled g and column labelled h , and also in the position that is in the row labelled h and column labelled g (as shown in Figure 45).

Proof In the Cayley table, the element in the row labelled g and column labelled h is $g \circ h$, and the element in the row labelled h and column labelled g is $h \circ g$.

Saying that both these elements are equal to e is the same as saying that $g \circ h = e = h \circ g$.

That is, it is equivalent to saying that h is an inverse of g . ■

Note that, in Proposition B7 and its proof above, g and h may be the *same* element, in which case the two positions mentioned are actually the same position, namely the position that is in the row labelled g and column labelled g , as shown in Figure 46. If e appears in this position then g (equal to h) is *self-inverse*, that is, the inverse of itself.

For convenience, here is a summary of what you have seen about identifying the inverses of elements from a Cayley table.

Identifying inverses from a Cayley table

- In a Cayley table for a set G and binary operation \circ on G with an identity element e :
- wherever e occurs on the main diagonal, the corresponding element in the table borders is self-inverse
 - wherever e occurs symmetrically with respect to the main diagonal, the corresponding elements in the table borders are inverses of each other.

These situations are illustrated in Figures 46 and 45, respectively.

The next worked exercise provides another demonstration of how to use a Cayley table to check the group axioms. In this worked exercise, the set and binary operation turn out not to form a group.

Worked Exercise B13

By using a Cayley table, determine whether (\mathbb{Z}_4, \times_4) is a group.

Solution

We construct a Cayley table for (\mathbb{Z}_4, \times_4) :

\times_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

We now check the group axioms.

G1 Closure

Every element in the body of the table is in \mathbb{Z}_4 , so \mathbb{Z}_4 is closed under multiplication.



G2 Associativity

Modular multiplication is associative.

G3 Identity

The row and column labelled 1 repeat the table borders, so 1 is an identity element for \times_4 on \mathbb{Z}_4 . (The table also shows that there is no other possible identity element.)

G4 Inverses

 Look for the occurrences of the identity element 1 in the body of the table. It does not occur at all in the row labelled 0, so there is no element $x \in \mathbb{Z}_4$ such that $0 \times_4 x = 1$. 

The identity element 1 does not occur in the row labelled 0, so 0 has no inverse.

Hence axiom G4 fails.

It follows that (\mathbb{Z}_4, \times_4) is not a group.

In general, for group axiom G4 (inverses) to be satisfied, each row must contain an occurrence of the identity element e (this ensures that for each element g there is an element h such that $g \circ h = e$), and this occurrence of e must either be on the main diagonal or appear symmetrically with another occurrence of e , with respect to the main diagonal (this ensures that whenever we have $g \circ h = e$, we also have $h \circ g = e$). (An alternative to checking that each row contains an occurrence of e is to check that each column does.)

The methods that you have seen for checking the group axioms from a Cayley table can be summarised as follows.

Using a Cayley table to check the group axioms

Let G be a finite set and let \circ be a binary operation defined on G . Then (G, \circ) is a group if and only if the Cayley table for (G, \circ) has the following properties.

- G1 Closure** The table contains only elements of the set G ; that is, no new elements appear in the body of the table.
- G2 Associativity** The operation \circ is associative.
(This property is not easy to check from a Cayley table.)
- G3 Identity** A row and a column labelled by the same element repeat the table borders. This element is an identity element, e say.
- G4 Inverses** Each row contains the identity element e , occurring either on the main diagonal or symmetrically with another occurrence of e , with respect to the main diagonal. (For each such occurrence of e , the corresponding elements in the table borders are inverses of each other.)

In the next exercise you can practise using Cayley tables to check the group axioms.

Exercise B21

By first constructing a Cayley table in each case, determine which of the following are groups.

- (a) $(\mathbb{Z}_5, +_5)$ (b) (\mathbb{Z}_5, \times_5)
- (c) $(\mathbb{Z}_5 - \{0\}, \times_5) = (\{1, 2, 3, 4\}, \times_5)$
- (d) $(\mathbb{Z}_6 - \{0\}, \times_6) = (\{1, 2, 3, 4, 5\}, \times_6)$
- (e) $(\{2, 4, 6, 8\}, \times_{10})$ (f) $(\{1, -1\}, \times)$

Now suppose that you are presented with a Cayley table with some abstract symbols in it, such as the following:

\circ	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

A Cayley table like this defines a set, namely the set of elements that appear in the table borders, and it defines a binary operation on that set, since the table tells us the result of composing any two elements of the set, in either order. So we can ask whether the set and the binary operation form a group.

As you have seen, you can use the Cayley table to check group axioms G1 (closure), G3 (identity) and G4 (inverses). For the Cayley table above, all the entries in the body of the table are elements of the original set $\{e, a, b, c, d\}$, so axiom G1 (closure) holds. Also, the row and column labelled by the element e repeat the table borders, so e is an identity element. That is, axiom G3 (identity) holds. Notice that e is the only possible identity element. The occurrences of the identity element in the body of the table tell us that e is self-inverse, that a and d are inverses of each other, and that b and c are inverses of each other. So axiom G4 (inverses) holds. That leaves just axiom G2 (associativity) to be checked. Unfortunately, there is no easy way to check this axiom, other than the obvious one of going through all the ways of combining three elements. If you were to do this (and it would take rather a long time!), then you would find that the binary operation defined by the Cayley table above is in fact associative. So the abstract Cayley table above is the Cayley table of a group.

However, it is possible for a Cayley table to satisfy axioms G1 (closure), G3 (identity) and G4 (inverses), but for the operation defined by the table *not* to be associative. Here is an example:

\circ	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

You can check in the usual ways that axioms G1 (closure), G3 (identity) and G4 (inverses) are all satisfied by this Cayley table. But axiom G2 (associativity) fails, because, for example, the two expressions $b \circ (c \circ d)$ and $(b \circ c) \circ d$ give different answers:

$$b \circ (c \circ d) = b \circ a = d,$$

$$(b \circ c) \circ d = a \circ d = b.$$

This example shows that you certainly cannot determine whether a given set and binary operation form a group only by using a Cayley table to help you check group axioms G1, G3 and G4. You do also need a means of checking group axiom G2 (associativity).

Exercise B22

Given that the binary operation \circ defined by the following Cayley table is associative, show that the set of elements in the table is a group under \circ .

\circ	a	b	c	d	e	f	g	h
a	f	e	g	h	a	b	d	c
b	e	f	h	g	b	a	c	d
c	h	g	f	e	c	d	b	a
d	g	h	e	f	d	c	a	b
e	a	b	c	d	e	f	g	h
f	b	a	d	c	f	e	h	g
g	c	d	a	b	g	h	f	e
h	d	c	b	a	h	g	e	f

Finally in this subsection, note that the definition of a group given in some other texts may look a little different from the definition that you have met in this module, even though the mathematical structure being defined is the same. In particular, in some texts our axiom G1 (closure) is part of the definition of a binary operation on a set, and hence is omitted from the list of group axioms.

You might also like to note that it can be proved that if group axioms G1 (closure) and G2 (associativity) hold for a set and binary operation (G, \circ) , then to check that group axioms G3 (identity) and G4 (inverses) also hold it is enough to show that

- there is an element e in G such that $g \circ e = g$ for all g in G , and
- for each element g in G , there is an element h in G such that $g \circ h = e$.

That is, you do not also have to show that $e \circ g = g$ for all g in G , or that for each element g in G the element h in G that satisfies $g \circ h = e$ also satisfies $h \circ g = e$. So the group axioms that you have met in this unit can be reduced to a more minimal set of axioms. However, in practice it is convenient to work with the set of group axioms stated earlier, and we will continue to do so throughout this module.

The origins of group theory

Group theory arose historically from three different areas of study: number theory, the theory of algebraic equations, and geometry.

The study of modular arithmetic that was introduced by Carl Friedrich Gauss in his *Disquisitiones Arithmeticae* of 1801 contains elements that we would nowadays recognise as group theory. At about the same time, many mathematicians, including Joseph-Louis Lagrange (1736–1813), Paolo Ruffini (1765–1822),

Augustin-Louis Cauchy (1789–1857) and Évariste Galois (1811–1832) worked on the question of which polynomial equations could be solved algebraically, and it gradually became apparent that the key to answering this question lay in considering groups of *permutations*, which you will meet in Unit B3 *Permutations*. In 1872, Felix Klein (1849–1925) in his *Erlangen Program*, a review of contemporary methods in geometry, used group theoretic methods to classify the different geometries, such as Euclidean, hyperbolic, and projective geometry, and a few years later Henri Poincaré (1854–1912) pioneered the introduction of group theoretic and geometric methods into complex function theory, these ideas becoming hugely significant in modern mathematics. One of the main instigators of the abstraction of the similar ideas in these different contexts into modern group theory was Arthur Cayley (1821–1895), around the middle of the 19th century.

In 1870 Camille Jordan (1838–1922) published his monumental treatise on permutation groups, and by around the end of the century textbooks on abstract group theory were being published, two of the most important being those by William Burnside and Heinrich Weber. Today, group theory remains a major area of mathematical research.

3.4 Standard groups of numbers

In this subsection you will meet some standard groups of numbers. They include many of the groups of numbers that you met in the previous two subsections.

Infinite groups of numbers

In Subsection 3.2 you saw that the sets \mathbb{Z} and \mathbb{R} , with addition, are groups, and that the sets \mathbb{Q}^* and \mathbb{R}^* , with multiplication, are groups. It can be shown in similar ways that the sets \mathbb{Q} and \mathbb{C} , with addition, are groups, and that the set \mathbb{C}^* , with multiplication, is a group. (As you may guess, the notation \mathbb{C}^* denotes the set $\mathbb{C} - \{0\}$ of all complex numbers except 0.)

In fact, you saw (without proof) in Unit A2 that the sets \mathbb{Q} , \mathbb{R} and \mathbb{C} , with addition and multiplication, are *fields*, and it follows from this that $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, (\mathbb{Q}^*, \times) , (\mathbb{R}^*, \times) and (\mathbb{C}^*, \times) are all groups. So we have the facts below.

Some standard infinite groups of numbers

The following are groups:

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +), \\ (\mathbb{Q}^*, \times), \quad (\mathbb{R}^*, \times), \quad (\mathbb{C}^*, \times).$$

Groups from modular arithmetic

In Worked Exercise B12 and Exercise B21 in Subsection 3.3 you saw that $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5, +_5)$ are groups. In fact, we have the following general result.

Theorem B8

For each integer $n \geq 2$, the set \mathbb{Z}_n is a group under $+_n$.

Proof The four group axioms hold because they are properties A1–A4 of addition in \mathbb{Z}_n , which you met in Subsection 3.3 of Unit A2. ■

You also saw in Exercise B21 that (\mathbb{Z}_5, \times_5) is not a group. In general, (\mathbb{Z}_n, \times_n) is not a group for any positive integer n , because 0 has no inverse with respect to \times_n . This type of situation has arisen before: you saw in Subsection 3.3 that (\mathbb{R}, \times) is not a group, because 0 has no inverse with respect to \times . You also saw that the set $\mathbb{R}^* = \mathbb{R} - \{0\}$ is a group under \times , and so are the sets $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ and $\mathbb{C}^* = \mathbb{C} - \{0\}$. However, removing the integer 0 from the set \mathbb{Z}_n does not necessarily give a group under \times_n : you saw in Exercise B21 that $(\{1, 2, 3, 4\}, \times_5)$ is a group, but $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group.

One reason why removing 0 from \mathbb{Z}_n does not necessarily give a group under \times_n is that, as you saw in Subsection 3.4 of Unit A2, in the set \mathbb{Z}_n only the integers coprime to n have inverses with respect to \times_n ; the other integers do not. So $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group because the integer 2, for instance, is not coprime to 6 and so does not have an inverse with respect to \times_6 in \mathbb{Z}_6 ; axiom G4 therefore fails. (Axiom G1 also fails: for example, $2, 3 \in \{1, 2, 3, 4, 5\}$, but $2 \times_6 3 = 0 \notin \{1, 2, 3, 4, 5\}$.)

It turns out, however, that if you remove not only the integer 0 from \mathbb{Z}_n , but also all the other integers in \mathbb{Z}_n that do not have inverses with respect to \times_n , then you *do* obtain a group under \times_n . This is proved below. The subset of \mathbb{Z}_n that you are left with is the set of all the integers in \mathbb{Z}_n that are coprime to n , and we denote this set by U_n . For example, the set of integers in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ that are coprime to 5 is

$$U_5 = \{1, 2, 3, 4\},$$

and this set forms a group under \times_n , as you saw in Exercise B21.

Similarly, the set of integers in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ that are coprime to 6 is

$$U_6 = \{1, 5\},$$

and this set forms a group under \times_6 . It has Cayley table

\times_6	1	5
1	1	5
5	5	1

and both of its elements are self-inverse. (The U in the notation U_n is for *units*, which means ‘elements that have multiplicative inverses’, but we will not need to use this term in this module.)

Here is the general result.

Theorem B9

For each integer $n \geq 2$, the set U_n of all integers in \mathbb{Z}_n that are coprime to n is a group under \times_n .

Proof We show that the four group axioms hold for (U_n, \times_n) . Throughout the proof, we make use of the properties of integers in \mathbb{Z}_n that you met in Unit A2.

G1 Closure

Let $a, b \in U_n$; then both a and b are coprime to n . To prove that $a \times_n b \in U_n$, we have to show that $a \times_n b$ is coprime to n .

To do this, we show that $a \times_n b$ has a multiplicative inverse in \mathbb{Z}_n . By Theorem A9 in Unit A2, since both a and b are coprime to n , they both have multiplicative inverses in \mathbb{Z}_n , say c and d , respectively. Now

$$(c \times_n d) \times_n (a \times_n b) = (c \times_n a) \times_n (d \times_n b) = 1 \times_n 1 = 1,$$

and similarly

$$(a \times_n b) \times_n (c \times_n d) = 1.$$

Hence $c \times_n d$ is a multiplicative inverse of $a \times_n b$ in \mathbb{Z}_n .

It now follows from Theorem A9 in Unit A2 that $a \times_n b$ is coprime to n , so $a \times_n b \in U_n$. Thus U_n is closed under \times_n .

G2 Associativity

Modular multiplication is associative.

G3 Identity

We have $1 \in U_n$, since 1 is coprime to n , and, for all $a \in U_n$,

$$a \times_n 1 = a = 1 \times_n a.$$

So 1 is an identity element for \times_n on U_n .

G4 Inverses

Let $a \in U_n$; then a is coprime to n . By Theorem A9 in Unit A2, a has a multiplicative inverse b in \mathbb{Z}_n . We have to show that $b \in U_n$; that is, we have to show that b is coprime to n . Since a and b satisfy the equations

$$a \times_n b = 1 = b \times_n a,$$

the number a is also a multiplicative inverse of b in \mathbb{Z}_n , and hence, also by Theorem A9 in Unit A2, b is coprime to n . So $b \in U_n$. Thus a has an inverse with respect to \times_n in U_n .

Hence (U_n, \times) satisfies the four group axioms, and so is a group. ■

If n is a prime number, then *all* the non-zero integers in \mathbb{Z}_n are coprime to n , so in this case simply removing the integer 0 from \mathbb{Z}_n *does* give a group. For example, $(\{1, 2, 3, 4\}, \times_5)$ is a group, as mentioned above, because 1, 2, 3 and 4 are all coprime to 5.

So Theorem B9 has the following corollary. In this corollary, and in general, we use the notation \mathbb{Z}_p^* to denote the set of all non-zero integers in \mathbb{Z}_p .

Corollary B10

If p is a prime number, then $(\mathbb{Z}_p^*, \times_p)$ is a group.

For example, $(\mathbb{Z}_5^*, \times_5)$, $(\mathbb{Z}_7^*, \times_7)$ and $(\mathbb{Z}_{19}^*, \times_{19})$ are groups, since 5, 7 and 19 are prime. Notice that, for any prime number p , the notations $(\mathbb{Z}_p^*, \times_p)$, (U_p, \times_p) and $(\{1, 2, \dots, p-1\}, \times_p)$ all denote the same group. However, we usually use the notation $(\mathbb{Z}_p^*, \times_p)$ when p is prime.

Note that, since $+_n$ and \times_n are commutative operations, all the groups described in Theorems B8 and B9, and in Corollary B10, are abelian.

Exercise B23

For each of the following groups, construct a Cayley table and write down the inverse of each element.

- (a) $(\mathbb{Z}_7, +_7)$ (b) $(\mathbb{Z}_7^*, \times_7)$ (c) (U_{10}, \times_{10}) (d) (U_9, \times_9)

Theorems B8 and B9 and Corollary B10 do not describe all the groups that come from modular arithmetic: there are many others. For example, in Exercise B21 you saw that $(\{2, 4, 6, 8\}, \times_{10})$ is a group; notice that this group does not contain the integer 1 and so its identity element is not 1.

4 Deductions from the group axioms

The advantage of defining a group (G, \circ) as a general set G and a general binary operation \circ on G that together satisfy the four group axioms G1–G4 is that anything that we can prove directly from the axioms (in the general case) must apply to any group (any specific case). Thus, by giving one proof, we can simultaneously establish a result that holds for groups of symmetries, infinite groups of real or complex numbers, modular arithmetic groups, and many more groups.

In this section you will meet some important basic properties of groups that can be deduced from the group axioms. The proofs in this section, showing how the deductions are made, are short and elegant. You should read them and try to understand them, to improve your knowledge of group theory and your understanding of how mathematical results are proved. However, be assured that a beginner in group theory is unlikely to think of these proofs unaided. Although you will be asked to prove some results in group theory yourself, and your understanding of the proofs in this section will help you with that, the proofs that you will be asked to produce will be more suitable for a beginner.

4.1 Basic properties of groups

Let us start with a reminder of the group axioms.

Definition

Let G be a set and let \circ be a binary operation defined on G . Then (G, \circ) is a **group** if the following four axioms hold.

G1 Closure For all g, h in G ,

$$g \circ h \in G.$$

G2 Associativity For all g, h, k in G ,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

G3 Identity There is an element e in G such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for \circ on G .)

G4 Inverses For each element g in G , there is an element h in G such that

$$g \circ h = e = h \circ g.$$

(The element h is an **inverse element** of g with respect to \circ .)

Before we go on to look at some deductions that we can make from the group axioms, it is important for you to understand what axiom G2 (associativity) tells us about the binary operation \circ of a group (G, \circ) .

It tells us that even though the binary operation of a group is a means of combining *two* group elements, we can write a composite of *three* group elements without using brackets. For example, if g, h and k are elements of a group (G, \circ) , then we can write

$$g \circ h \circ k,$$

rather than either

$$(g \circ h) \circ k \quad \text{or} \quad g \circ (h \circ k).$$

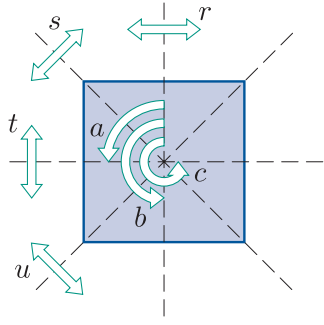


Figure 47 $S(\square)$

This is because axiom G2 guarantees that both possible interpretations of $g \circ h \circ k$ give the same answer. We can evaluate $g \circ h \circ k$ by using either interpretation.

You saw this illustrated for the group $S(\square)$ in Subsection 1.2: you saw there that, with our standard labelling for the symmetries of the square (shown again in Figure 47), we can evaluate the composite $b \circ a \circ t$ in either of the following two ways, obtaining the same answer:

$$\begin{aligned} b \circ (a \circ t) &= b \circ u = s, \\ (b \circ a) \circ t &= c \circ t = s. \end{aligned}$$

In fact axiom G2 tells us more: it tells us that we can write a composite of *any finite number* of group elements with no brackets, without there being any ambiguity about the meaning of the expression. For example, if a , b , c and d are elements of a group (G, \circ) , then we can write the composite

$$a \circ b \circ c \circ d$$

of four group elements without brackets. To see why, notice that there are various ways in which we can ‘bracket’ this expression to indicate which elements are being composed with which, such as

$$\begin{aligned} (a \circ b) \circ (c \circ d), \\ a \circ (b \circ (c \circ d)), \\ a \circ ((b \circ c) \circ d), \\ (a \circ (b \circ c)) \circ d, \end{aligned}$$

and so on. The first two expressions here are equal, because applying axiom G2 to the three group elements a , b and $c \circ d$ (in that order) gives

$$(a \circ b) \circ (c \circ d) = a \circ (b \circ (c \circ d)).$$

Similarly, the second and third expressions are equal, because applying axiom G2 to the three group elements b , c and d (in that order) gives

$$a \circ (b \circ (c \circ d)) = a \circ ((b \circ c) \circ d).$$

In this manner, by repeatedly applying axiom G2, we can show that any way of bracketing the expression is equal to any other way. So all the different ways of bracketing the expression give the same answer, and hence we can write the expression with no brackets, without there being any ambiguity about its meaning.

We can evaluate a composite of group elements such as $a \circ b \circ c \circ d$ by bracketing it however we wish, *provided that we do not change the order in which the elements appear*.

Now let us look at some of the basic properties of groups that can be deduced from the group axioms.

Uniqueness properties

Each of the examples of groups that you have seen has contained precisely *one* identity element. In fact this is always the case, as stated and proved below. We say that the identity element in a group is *unique*.

There is a standard method that is often helpful for proving uniqueness, and we use it in the proof below. The idea is that, to prove that there can be only one identity element in a group, we suppose that e and e' , say, both represent identity elements, and prove that the only possibility is that e and e' are in fact the same element. You can often use a similar technique to prove uniqueness in other situations, and in fact we will use the same technique in the next proof too.

Proposition B11

In any group, the identity element is unique.

Proof Let (G, \circ) be a group, and suppose that e and e' are identity elements in this group. We have to show that $e = e'$.

Consider the expression $e \circ e'$. Since e is an identity element, the result of composing e with any other element, in either order, is simply that other element (by axiom G3). So we must have

$$e \circ e' = e'.$$

Similarly, since e' is an identity element, we must have

$$e \circ e' = e.$$

It follows that

$$e = e',$$

as required. ■

Because of Proposition B11, we can, and shall, refer to *the* identity element of a group.

We now look at another uniqueness property. In each of the examples of groups that you have seen, every element has precisely one inverse. Again, this is always the case in a group, as proved below.

Proposition B12

In any group, each element has a unique inverse.

Proof Let (G, \circ) be a group with identity element e , let g be any element in this group, and suppose that g has inverse elements x and y . We have to show that $x = y$.

Consider the expression $y \circ g \circ x$. Since x is an inverse of g , we have

$$\begin{aligned} y \circ g \circ x &= y \circ (g \circ x) \quad (\text{by axiom G2, associativity}) \\ &= y \circ e \quad (\text{by axiom G4, inverses}) \\ &= y \quad (\text{by axiom G3, identity}). \end{aligned}$$

On the other hand, since y is an inverse of g , we have

$$\begin{aligned} y \circ g \circ x &= (y \circ g) \circ x \quad (\text{by axiom G2, associativity}) \\ &= e \circ x \quad (\text{by axiom G4, inverses}) \\ &= x \quad (\text{by axiom G3, identity}). \end{aligned}$$

It follows that $x = y$, as required. ■

Because of Proposition B12, we can, and shall, refer to *the* inverse of a group element. This property also allows us to use the following notation for inverses in a group.

Notation

Let g be an element of a group (G, \circ) . Then we denote the inverse of g by g^{-1} . So

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

In fact, the two proofs above are not the first time that you have met the standard method for proving uniqueness. For example, you saw in Unit A1 how to use this method to prove that a function is one-to-one. To prove that a function f is one-to-one, essentially you have to show that for every element y in the image set of f , there is a *unique* element x in the domain of f such that $f(x) = y$. You saw that to do this, the standard method is to suppose that x_1 and x_2 , say, both represent elements that are mapped by f to y , and prove that the only possibility is that x_1 and x_2 are in fact the same element.

Also, in Unit A2 the standard method for proving uniqueness was used to prove that, in the system \mathbb{Z}_n with addition and multiplication modulo n , if an element *has* a multiplicative inverse then that multiplicative inverse is unique. The proof of that result is essentially the same as the proof of Proposition B12 above.

Properties of inverse elements

We now turn to some properties of inverse elements in groups.

In the examples of groups that you have seen, some elements are self-inverse, and the remaining elements can be arranged into pairs of elements that are inverses of each other. So, in all the examples, if g is a group element with inverse g^{-1} , then the inverse of g^{-1} is g . This is always the case in a group, as stated and proved below.

Proposition B13

Let g be an element of a group (G, \circ) . Then

the inverse of g^{-1} is g ,

that is,

$$(g^{-1})^{-1} = g.$$

Proof By axiom G4, since g has inverse g^{-1} ,

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

We can write these equations in a different order as

$$g^{-1} \circ g = e = g \circ g^{-1}.$$

This tells us that g is an inverse of g^{-1} . Hence, by Proposition B12 (uniqueness of the inverse of a group element), g is *the* inverse of g^{-1} ; that is, we have

$$(g^{-1})^{-1} = g. \quad \blacksquare$$

Our second property of inverses concerns the inverse of a composite of two group elements.

Proposition B14

Let x and y be elements of a group (G, \circ) . Then

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

Proof We start by showing that $y^{-1} \circ x^{-1}$ is an inverse of $x \circ y$. To do this, we have to show that

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = e = (y^{-1} \circ x^{-1}) \circ (x \circ y).$$

Now

$$\begin{aligned}
 (x \circ y) \circ (y^{-1} \circ x^{-1}) &= x \circ (y \circ y^{-1}) \circ x^{-1} \\
 &\quad \text{(by axiom G2, associativity)} \\
 &= x \circ e \circ x^{-1} \quad \text{(by axiom G4, inverses)} \\
 &= x \circ x^{-1} \quad \text{(by axiom G3, identity)} \\
 &= e \quad \text{(by axiom G4, inverses),}
 \end{aligned}$$

and

$$\begin{aligned}
 (y^{-1} \circ x^{-1}) \circ (x \circ y) &= y^{-1} \circ (x^{-1} \circ x) \circ y \\
 &\quad \text{(by axiom G2, associativity)} \\
 &= y^{-1} \circ e \circ y \quad \text{(by axiom G4, inverses)} \\
 &= y^{-1} \circ y \quad \text{(by axiom G3, identity)} \\
 &= e \quad \text{(by axiom G4, inverses).}
 \end{aligned}$$

Hence $y^{-1} \circ x^{-1}$ is an inverse of $x \circ y$. So, by Proposition B12 (uniqueness of the inverse of a group element), $y^{-1} \circ x^{-1}$ is *the* inverse of $x \circ y$; that is,

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}. \quad \blacksquare$$

Proposition B14 is a general property that holds for all inverses of composites (not just in group theory). For example, if f and g are functions that have inverses (that is, if they are one-to-one functions), then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Here is one way to see that the different orders of composition on the two sides of equations like this makes sense. Consider the composite action of first putting your socks on and then putting your shoes on. To carry out the inverse of this action, you first take your shoes off and then take your socks off!

Proposition B14 extends to composites of more than two group elements. For example, if x , y and z are elements of a group (G, \circ) , then

$$(x \circ y \circ z)^{-1} = z^{-1} \circ y^{-1} \circ x^{-1}.$$

This follows from Proposition B14, as follows:

$$\begin{aligned}
 (x \circ y \circ z)^{-1} &= (y \circ z)^{-1} \circ x^{-1} \quad \text{(by Proposition B14)} \\
 &= z^{-1} \circ y^{-1} \circ x^{-1} \quad \text{(by Proposition B14 again).}
 \end{aligned}$$

By repeatedly applying Proposition B14 in this way, we can extend it to a composite of any finite number of group elements.

Our final properties in this subsection, in the box below, do not explicitly involve inverses, but are proved using inverses. These properties will be familiar to you from elementary arithmetic, in the cases where the binary operation is addition or multiplication. For example, suppose that a and b are real numbers, and that $a + 3 = b + 3$. Both sides of this equation involve adding the same real number (here, 3) to another real number, so we know that we can *cancel* the 3 that occurs on both sides of the equation and conclude that $a = b$. Similarly, if $5a = 5b$ we can cancel the 5 that multiplies the real numbers a and b , and again conclude that $a = b$.

These properties are known as *cancellation laws*. They apply in any group, as stated below.

Proposition B15 Cancellation Laws

In any group (G, \circ) with elements a, b and x :

- if $x \circ a = x \circ b$, then $a = b$ (**Left Cancellation Law**)
- if $a \circ x = b \circ x$, then $a = b$ (**Right Cancellation Law**).

Proof Here is a proof of the Left Cancellation Law. Suppose that, in a group (G, \circ) ,

$$x \circ a = x \circ b.$$

Composing both sides on the left with the inverse of x , we obtain

$$x^{-1} \circ x \circ a = x^{-1} \circ x \circ b.$$

By axiom G2 (associativity), this gives

$$(x^{-1} \circ x) \circ a = (x^{-1} \circ x) \circ b.$$

Hence, by axiom G4 (inverses), we obtain

$$e \circ a = e \circ b,$$

and therefore, by axiom G3 (identity),

$$a = b.$$

You are asked to prove the Right Cancellation Law in the next exercise. ■

Exercise B24

By adapting the proof above, prove the Right Cancellation Law for a group (G, \circ) , namely,

$$\text{if } a \circ x = b \circ x, \text{ then } a = b.$$

In the next two exercises, you can try your hand at proving results by using the group axioms. Do not worry if you find these exercises difficult: accept them as a challenge. Proving results in group theory can be tricky, especially when you are new to it, and there are further opportunities for you to practise it throughout Book B.

Exercise B25

Suppose that a, b and c are elements of a group (G, \circ) such that $a \circ b \circ c = e$, where e is the identity element. Prove that $b \circ c \circ a = e$.

As you become more familiar with proving results in group theory, you do not need to name the group axioms explicitly every time you use them: you just need to make sure that you clearly justify the steps of your proof, using appropriate words. Your justification of a step might involve referring to a group axiom in some way, or it might be based on a result proved earlier about groups. And, of course, it may be based on something else altogether, such as a supposition that you made in order to prove an implication. In general, the amount of justification that you provide should be enough to convince a reader whose mathematical experience is about the same as yours. This will be similar to the amount of justification in comparable proofs given in the module texts and in the solutions to exercises and worked exercises.

The next exercise is a little more challenging than the one above. Treat it as a puzzle: see if you can work it out, but do not worry if you cannot.

Exercise B26

Let (G, \circ) be a group. Proposition B14 tells us that

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1} \text{ for all } x, y \in G.$$

Prove that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G$$

if and only if (G, \circ) is abelian. You can use any of the properties proved so far in this section.

Hint. Remember from Unit A3 *Mathematical language* that to prove a statement of the form ‘ A if and only if B ’, you have to prove both that A implies B and that B implies A .

Remember also that an *abelian* group (G, \circ) is one for which $x \circ y = y \circ x$ for all $x, y \in G$.

4.2 Properties of group tables

The Cayley table of a group is called a **group table**. In this subsection we will look at some properties possessed by every group table.

In Subsection 3.3 you met some properties of group tables that correspond directly to the group axioms. For example, you saw that group axioms G1 (closure) and G3 (identity) immediately give the following two properties.

Proposition B16

In a group table, the only elements in the body of the table are those that appear in the table borders.

Proposition B17

In a group table, the row and column corresponding to the identity element repeat the table borders.

Exercise B27

Decide which is the identity element in each of the following group tables.

(a)

	O	E
O	E	O
E	O	E

(b)

	D	I
D	D	I
I	I	D

(c)

	u	v	w	x
u	w	x	u	v
v	x	w	v	u
w	u	v	w	x
x	v	u	x	w

As you have seen, if we know which element of a group is the identity element, then we usually write this element first in the borders of the group table.

Here is another property of group tables.

Proposition B18

In a group table, each element of the group occurs exactly once in each row and exactly once in each column.

Proof We prove this statement for the rows of a group table. The proof for columns is similar, and you are asked to produce it in the next exercise.

Let g be any group element; we will consider the row corresponding to g . Let h also be any group element; we will show that h occurs exactly once in this row.

This is equivalent to proving that there is *exactly one* element of the group, x say, such that

$$g \circ x = h,$$

as illustrated in Figure 48.

To show that there is *at least* one such element x , let $x = g^{-1} \circ h$. Then

$$\begin{aligned} g \circ x &= g \circ g^{-1} \circ h \\ &= e \circ h \\ &= h, \end{aligned}$$

so $x = g^{-1} \circ h$ has the property $g \circ x = h$, as claimed.

To show that $x = g^{-1} \circ h$ is the *only* element x of the group such that $g \circ x = h$, we use our standard method for proving uniqueness. Suppose that x and y are group elements such that

$$g \circ x = h \quad \text{and} \quad g \circ y = h.$$

	\cdots	x	\cdots
\vdots			
g	\cdots	h	\cdots
\vdots			

Figure 48 Element h in row g

Then

$$g \circ x = g \circ y,$$

so, by the Left Cancellation Law,

$$x = y.$$

So there is indeed exactly one element x of the group such that $g \circ x = h$, namely $x = g^{-1} \circ h$.

In other words, in the row labelled g , the element h appears exactly once; it appears in the column labelled by the element $g^{-1} \circ h$. ■

Exercise B28

By adapting the proof above, prove the second part of Proposition B18; that is, prove that in a group table each element of the group occurs exactly once in each column.

Proposition B18 tells us, in particular, that the identity element e occurs exactly once in each row and each column of a group table. By what you saw in Subsection 3.3 about checking the group axioms from a Cayley table, this single occurrence of e in each row (or column) must appear either on the main diagonal or symmetrically with another occurrence of e , with respect to the main diagonal, as illustrated in Figure 49.

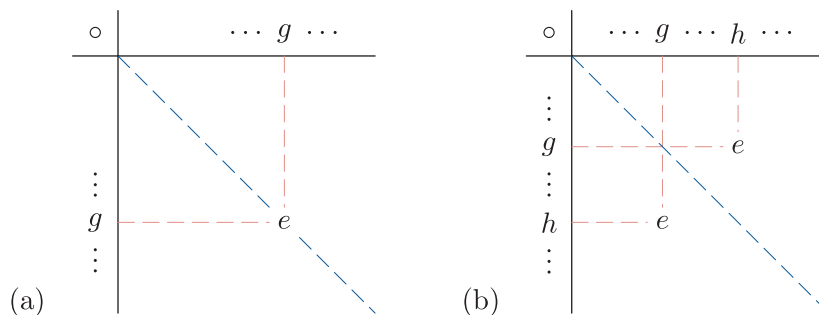


Figure 49 The occurrence of the identity element e in row g (a) if g is self-inverse (b) if g has inverse $h \neq g$

So *all* occurrences of the identity element e in a group table must appear symmetrically with respect to the main diagonal. This property is stated slightly more concisely below.

Proposition B19

In a group table, the identity element e occurs symmetrically with respect to the main diagonal.

Exercise B29

In each of the Cayley tables below, the identity element e occurs in each row and column, but the table is not a group table. Explain how you can tell this.

(a)	\circ	e	a	b	c	d
	e	e	a	b	c	d
	a	a	b	d	e	c
	b	b	e	c	d	a
	c	c	d	e	a	b
	d	d	c	a	b	e

(b)	\circ	e	a	b	c	d
	e	e	a	b	c	d
	a	a	b	d	e	c
	b	b	d	c	d	e
	c	c	e	d	a	b
	d	d	c	e	b	a

Finally in this subsection, we consider a property that *only some* group tables have.

Notice that, for any elements g and h of a group G , the entries in the group table corresponding to the composites $g \circ h$ and $h \circ g$ are placed symmetrically with respect to the main diagonal, as illustrated in Figure 50. Thus we have the following result.

Proposition B20 Group table of an abelian group

A group is abelian if and only if its group table is symmetric with respect to the main diagonal.

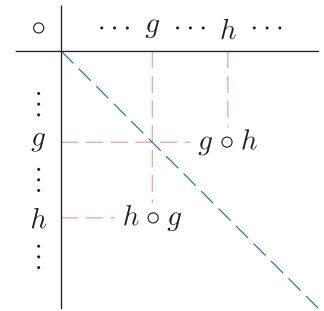


Figure 50 The positions of the composites $g \circ h$ and $h \circ g$ in a group table

For example, Figure 51 shows that $(\mathbb{Z}_6, +_6)$ is an abelian group, whereas $(S(\triangle), \circ)$ is not.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

(a) symmetric

(b) not symmetric

Figure 51 The group tables of (a) $(\mathbb{Z}_6, +_6)$ (b) $(S(\triangle), \circ)$

Exercise B30

Each of the following tables is a group table for a group of order 8 with identity e . In each case, state whether the group is abelian and draw up a table of inverses.

(a)	<table><tr><th></th><th>e</th><th>a</th><th>b</th><th>c</th><th>d</th><th>f</th><th>g</th><th>h</th></tr><tr><th>e</th><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td></tr><tr><th>a</th><td>a</td><td>e</td><td>c</td><td>b</td><td>f</td><td>d</td><td>h</td><td>g</td></tr><tr><th>b</th><td>b</td><td>c</td><td>e</td><td>a</td><td>g</td><td>h</td><td>d</td><td>f</td></tr><tr><th>c</th><td>c</td><td>b</td><td>a</td><td>e</td><td>h</td><td>g</td><td>f</td><td>d</td></tr><tr><th>d</th><td>d</td><td>f</td><td>g</td><td>h</td><td>e</td><td>a</td><td>b</td><td>c</td></tr><tr><th>f</th><td>f</td><td>d</td><td>h</td><td>g</td><td>a</td><td>e</td><td>c</td><td>b</td></tr><tr><th>g</th><td>g</td><td>h</td><td>d</td><td>f</td><td>b</td><td>c</td><td>e</td><td>a</td></tr><tr><th>h</th><td>h</td><td>g</td><td>f</td><td>d</td><td>c</td><td>b</td><td>a</td><td>e</td></tr></table>		e	a	b	c	d	f	g	h	e	e	a	b	c	d	f	g	h	a	a	e	c	b	f	d	h	g	b	b	c	e	a	g	h	d	f	c	c	b	a	e	h	g	f	d	d	d	f	g	h	e	a	b	c	f	f	d	h	g	a	e	c	b	g	g	h	d	f	b	c	e	a	h	h	g	f	d	c	b	a	e	(b)	<table><tr><th></th><th>e</th><th>a</th><th>b</th><th>c</th><th>d</th><th>f</th><th>g</th><th>h</th></tr><tr><th>e</th><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td></tr><tr><th>a</th><td>a</td><td>b</td><td>c</td><td>e</td><td>f</td><td>g</td><td>h</td><td>d</td></tr><tr><th>b</th><td>b</td><td>c</td><td>e</td><td>a</td><td>g</td><td>h</td><td>d</td><td>f</td></tr><tr><th>c</th><td>c</td><td>e</td><td>a</td><td>b</td><td>h</td><td>d</td><td>f</td><td>g</td></tr><tr><th>d</th><td>d</td><td>h</td><td>g</td><td>f</td><td>b</td><td>a</td><td>e</td><td>c</td></tr><tr><th>f</th><td>f</td><td>d</td><td>h</td><td>g</td><td>c</td><td>b</td><td>a</td><td>e</td></tr><tr><th>g</th><td>g</td><td>f</td><td>d</td><td>h</td><td>e</td><td>c</td><td>b</td><td>a</td></tr><tr><th>h</th><td>h</td><td>g</td><td>f</td><td>d</td><td>a</td><td>e</td><td>c</td><td>b</td></tr></table>		e	a	b	c	d	f	g	h	e	e	a	b	c	d	f	g	h	a	a	b	c	e	f	g	h	d	b	b	c	e	a	g	h	d	f	c	c	e	a	b	h	d	f	g	d	d	h	g	f	b	a	e	c	f	f	d	h	g	c	b	a	e	g	g	f	d	h	e	c	b	a	h	h	g	f	d	a	e	c	b
	e	a	b	c	d	f	g	h																																																																																																																																																													
e	e	a	b	c	d	f	g	h																																																																																																																																																													
a	a	e	c	b	f	d	h	g																																																																																																																																																													
b	b	c	e	a	g	h	d	f																																																																																																																																																													
c	c	b	a	e	h	g	f	d																																																																																																																																																													
d	d	f	g	h	e	a	b	c																																																																																																																																																													
f	f	d	h	g	a	e	c	b																																																																																																																																																													
g	g	h	d	f	b	c	e	a																																																																																																																																																													
h	h	g	f	d	c	b	a	e																																																																																																																																																													
	e	a	b	c	d	f	g	h																																																																																																																																																													
e	e	a	b	c	d	f	g	h																																																																																																																																																													
a	a	b	c	e	f	g	h	d																																																																																																																																																													
b	b	c	e	a	g	h	d	f																																																																																																																																																													
c	c	e	a	b	h	d	f	g																																																																																																																																																													
d	d	h	g	f	b	a	e	c																																																																																																																																																													
f	f	d	h	g	c	b	a	e																																																																																																																																																													
g	g	f	d	h	e	c	b	a																																																																																																																																																													
h	h	g	f	d	a	e	c	b																																																																																																																																																													

5 Symmetry in \mathbb{R}^3

Having considered symmetries of two-dimensional figures, and seen that they form groups, we now extend the ideas to three-dimensional objects. Remember that we use the notation \mathbb{R}^3 to denote three-dimensional space, in which a point is specified by three coordinates x, y, z .

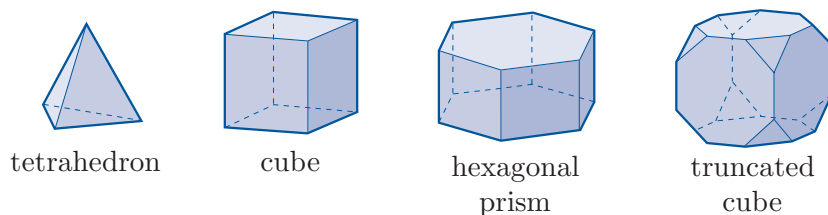
5.1 Symmetries of figures in \mathbb{R}^3

We begin by adapting to \mathbb{R}^3 the definitions that you met earlier relating to figures and symmetries in \mathbb{R}^2 .

Definitions

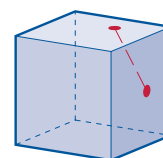
- A **figure** in \mathbb{R}^3 is any subset of \mathbb{R}^3 .
- A **bounded** figure in \mathbb{R}^3 is one that can be surrounded by a sphere (of finite radius).

A figure in \mathbb{R}^3 that is a shape with non-zero height, non-zero width and non-zero depth is called a **solid figure**, or just a **solid**. In this section we will mainly consider bounded solids whose faces are polygons. A solid of this type is called a **polyhedron**; some examples are shown in Figure 52. The plural of *polyhedron* is *polyhedra* or simply *polyhedrons*.

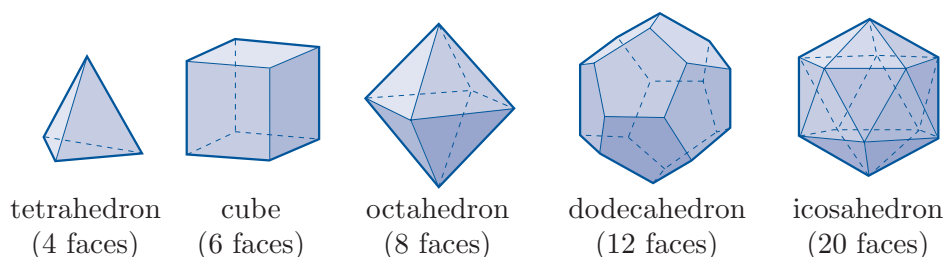
**Figure 52** Four polyhedra

The word *polyhedron* derives from the Greek for ‘many faces’. Similarly, the word *polygon* derives from the Greek for ‘many angles’.

We will restrict our attention to **convex** polyhedra; that is, those without dents or dimples or spikes – in other words, those that are such that if you choose any two points that lie on different faces, then the line segment joining those points always lies inside the polyhedron, as illustrated in Figure 53.

**Figure 53** A cube is a convex polyhedron

Of particular interest are the **regular polyhedra (Platonic solids)**: these are the convex polyhedra in which all the faces are congruent regular polygons and at each vertex the same number of faces meet, arranged in the same way. (Remember that two plane figures are said to be **congruent** if they are the same size and shape – that is, if you can translate, rotate and/or reflect one figure to make it fit exactly on top of the other.) There are five regular polyhedra, as shown in Figure 54. An explanation of why there are only five is given in Subsection 5.4.

**Figure 54** The five Platonic solids

The Platonic solids are so named not because Plato (427–347 BCE) discovered them, but because he associated the regular tetrahedron, cube, octahedron and icosahedron with the four elements of fire, earth, air and water, respectively; it is not completely clear with what Plato associated the dodecahedron, but he said that it ‘delineates the whole’.

The definitions of an isometry and a symmetry for \mathbb{R}^3 are almost exactly the same as for \mathbb{R}^2 .

Definitions

An **isometry** of \mathbb{R}^3 is a function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ that preserves distances.

A **symmetry** of a figure F in \mathbb{R}^3 is an isometry that maps F to itself; that is, an isometry $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ such that $f(F) = F$.

Two symmetries of a figure F are **equal** if they have the same effect on F , that is, $f(X) = g(X)$ for all points $X \in F$.

The types of isometries that are potential symmetries of a bounded figure in \mathbb{R}^3 are the following.

- The **identity transformation**: equivalent to doing nothing to a figure.
- A **rotation**: as illustrated in Figure 55(a), it is specified by a line known as an *axis of symmetry* together with a *direction* of rotation and an *angle of rotation*.
- A **reflection**: as illustrated in Figure 55(b), it is specified by the *plane* in which the reflection takes place.
- A **composite** of isometries of the types above – which may itself be of one of the types above, or (unlike with symmetries of plane figures) may not.

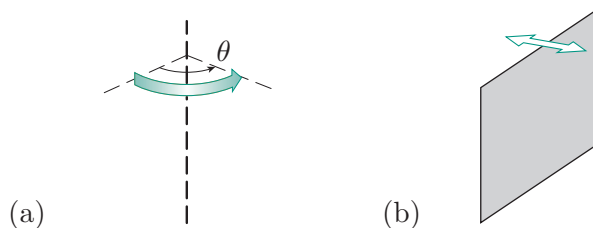


Figure 55 (a) A rotation about an axis of symmetry (b) A reflection in a plane

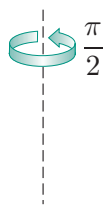


Figure 56 An arrow indicating the direction of rotation, with the angle of rotation marked

We have to be careful with rotations in \mathbb{R}^3 , as what is clockwise when we look along a line in one direction is anticlockwise when we look along it in the other direction. We often indicate the direction of rotation by an arrow on a diagram, as in Figure 55(a). However, note that in the remainder of this section a rotation arrow in a diagram of a figure in \mathbb{R}^3 indicates only the *direction of rotation*, as illustrated in Figure 56, and not the *size of the angle* through which the figure is rotated. The size of the angle of rotation is sometimes marked next to the rotation arrow, as in Figure 56.

To illustrate symmetries of figures in \mathbb{R}^3 , let us consider some symmetries of the cube.

Figure 57 shows the effect of a particular rotational symmetry of the cube, namely rotation through $\pi/2$ about the vertical line through the centre of the cube, in the direction indicated.

In diagrams such as this, the numbers have a similar purpose to the numbers that we used in diagrams of plane figures earlier. They do not label vertices: instead they label fixed locations in space, so they do not move when the figure is rotated or reflected, or transformed in any other way by a symmetry. In Figure 57, and in the next few figures, the change in the position of the cube is indicated by a dot and a small square that mark two corners of one of its faces.

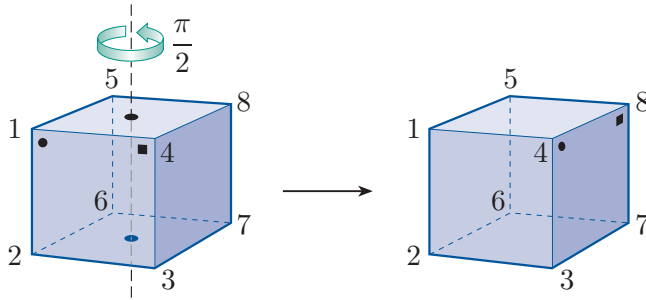


Figure 57 A rotation of the cube through $\pi/2$ about its vertical axis

We use two-line symbols to represent symmetries of figures in \mathbb{R}^3 in the same way as we do for plane figures. For example, with the labelling shown, the symmetry in Figure 57 is represented by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 8 & 1 & 2 & 6 & 5 \end{pmatrix}.$$

Another symmetry of the cube is the identity symmetry, which can be thought of as a zero rotation, and is represented by

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}.$$

Figure 58 shows a reflectional symmetry of the cube, namely reflection in the vertical plane shown.

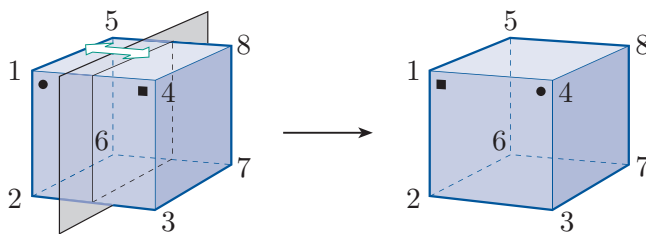


Figure 58 A reflection of the cube in a vertical plane

The two-line symbol for this reflection is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{pmatrix}.$$

We can compose symmetries of solid figures written in two-line notation in the same way as for plane figures.

For example, the rotation in Figure 57 followed by the reflection in Figure 58 is the symmetry

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 8 & 1 & 2 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 6 & 5 & 4 & 3 & 7 & 8 \end{pmatrix}.$$

(Remember that the symmetry on the right is the one carried out first.)

This symmetry is reflection in the diagonal plane passing through the locations labelled 1, 2, 7 and 8, as shown in Figure 59.

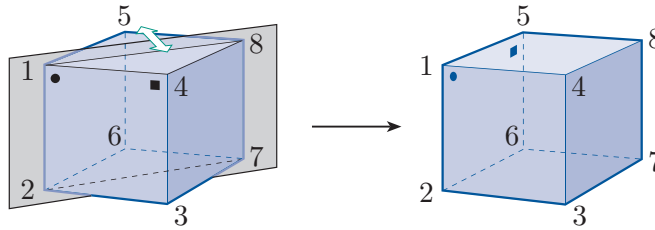


Figure 59 A reflection of the cube in a diagonal vertical plane

We can also find the inverse of a symmetry of a solid figure written in two-line notation in the same way as for plane figures.

For example, for the rotation in Figure 57, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 8 & 1 & 2 & 6 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 3 & 7 & 8 & 1 & 2 & 6 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} \\ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 2 & 1 & 8 & 7 & 3 & 4 \end{pmatrix}.$$

This is the rotation of the cube through $3\pi/2$ about the vertical line through the centre, in the direction indicated in Figure 60.

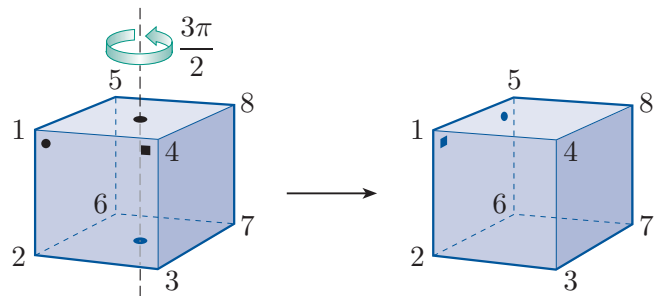


Figure 60 A rotation of the cube through $3\pi/2$ about its vertical axis

For any figure F , we denote the set of symmetries of F by $S(F)$. You saw earlier that if F is a plane figure, then $S(F)$ is a group under function composition. The arguments that confirmed this remain valid if F is a figure in \mathbb{R}^3 , as you might like to check. So we have the following general result.

Theorem B21

If F is a figure (in \mathbb{R}^2 or \mathbb{R}^3), then $S(F)$ forms a group under function composition.

For any figure F , the group $(S(F), \circ)$ is called the **symmetry group**

Direct and indirect symmetries of a figure in \mathbb{R}^3

In Subsection 1.1 we demonstrated the symmetries of the square in \mathbb{R}^2 by using a paper model. You saw that we could demonstrate rotations of the square by moving the paper model within the plane, but that to demonstrate reflections we needed to ‘flip’ the paper square about an axis of symmetry.

For figures in \mathbb{R}^3 , the only symmetries that we can demonstrate physically with a model are rotations. We cannot flip our model to demonstrate a reflection, as we did for the square – to do that, we would need access to a fourth dimension!

The symmetries of a figure in \mathbb{R}^3 that we can demonstrate with a model (that is, rotations) are called **direct** symmetries, whereas those that we cannot show physically with the model are called **indirect** symmetries.

For a polyhedron or any other figure in \mathbb{R}^3 , we can imagine (or, if practicable, make) a *second* model to represent the reflected figure. You can think of this second model as the three-dimensional equivalent of the other side of a paper model of a plane figure, since the other side of the paper model is a model of the reflected plane figure. Earlier we shaded the model of the reflected plane figure a darker colour to distinguish it from the model of the original plane figure, and you might like to think of the model of the reflected figure in \mathbb{R}^3 as shaded darker too, to distinguish it from the original model.

As in the case of plane figures, composition of direct and indirect symmetries of figures in \mathbb{R}^3 follows a standard pattern, as follows.

direct \circ direct = direct	\circ	direct	indirect
direct \circ indirect = indirect	direct	direct	indirect
indirect \circ direct = indirect	indirect	indirect	direct
indirect \circ indirect = direct			

Also, as before, the inverse of a direct symmetry is a direct symmetry, and the inverse of an indirect symmetry is an indirect symmetry.

You also saw earlier that if F is a plane figure that has a finite number of symmetries, then either all the symmetries of F are direct symmetries, or half of the symmetries are direct and half are indirect. This is also true for figures in \mathbb{R}^3 .

To see this, consider a figure F in \mathbb{R}^3 , and suppose that it has n direct symmetries. In other words, there are n different ways to pick up a model of the figure and replace it to occupy the same space, but possibly with its vertices at different locations. If F has *no* indirect symmetries, then these n direct symmetries are the only symmetries of F . Now suppose that F has at least one indirect symmetry. This means that you can remove the model of F and replace it with the model of the reflected version of F , to occupy the same space. Once you have done that, there must be n different ways to pick up the reflected model again and replace it to occupy the same space. In other words, F has n indirect symmetries, and if you choose any one of them, then you can obtain all n of them by composing the one that you chose with each of the n direct symmetries in turn. (In other words, they can all be illustrated by rotating the second model of the polyhedron.) So we have the following general result.

Theorem B22

If a figure (either a plane figure or a figure in \mathbb{R}^3) has a finite number of symmetries, then either

- all the symmetries are direct, or
- half of the symmetries are direct and half are indirect.

If there are indirect symmetries, then they can all be obtained by composing any single indirect symmetry with all of the direct symmetries.

We denote the set of direct symmetries of a figure F by $S^+(F)$.

5.2 Counting the symmetries of a polyhedron

Finding all the symmetries of a polyhedron is generally more tricky than finding all the symmetries of a plane figure such as a polygon. It is usually helpful to start by working out the *number of symmetries* that the polyhedron has. In this subsection you will see how to do this, and in the next subsection we will look at how you might go about actually finding the symmetries. We will start with the regular polyhedra.

Counting the symmetries of a regular polyhedron

As an example, let us try to count the symmetries of the simplest regular polyhedron, the tetrahedron, shown in Figure 61. In Figure 61, the lowest face of the tetrahedron is labelled as its *base*.

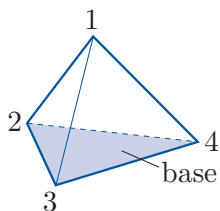


Figure 61 A tetrahedron

Imagine picking up the tetrahedron, and placing it down again to occupy the same space that it occupied originally, but possibly with the vertices at new locations. Let us count the number of ways of doing this. We can choose any of the four faces to be the base, and then there are three ways of placing the tetrahedron on this base, corresponding to the three rotational symmetries of the base triangle. Thus altogether there are $4 \times 3 = 12$ ways of placing the tetrahedron down again. Hence the tetrahedron has 12 direct symmetries. (One of them is the identity symmetry.)

The tetrahedron also has indirect symmetries – for example, a reflection in the vertical plane through the edge joining the vertices at locations 1 and 3 and the midpoint of the edge joining the vertices at locations 2 and 4, as shown in Figure 62.

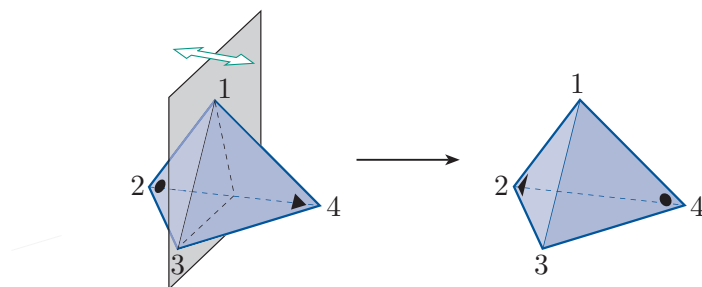


Figure 62 A reflectional symmetry of the tetrahedron

We know that if a figure with a finite number of symmetries has indirect symmetries, then it must have the same number of indirect symmetries as direct symmetries. It follows that the tetrahedron has 12 indirect symmetries, and hence it has 24 symmetries altogether.

Here is another way to work out that the tetrahedron has 24 symmetries. We count the number of ways of replacing the tetrahedron *or the reflected tetrahedron* in the space occupied originally by the tetrahedron, but possibly with the vertices at new locations. We can choose any of the four faces to be placed as the base. Now consider the symmetries of the base. It is an equilateral triangle, so it has six symmetries. Imagine applying any one of these symmetries to the base, and allowing the rest of the tetrahedron to be transformed accordingly. For example, if we rotate the base about its centre, then the whole tetrahedron is rotated about the vertical line through this point, as shown in Figure 63(a). Similarly, if we reflect the base in a line that goes through a vertex and the midpoint of the opposite edge, then the whole tetrahedron is reflected in the vertical plane that passes through this line, as shown in Figure 63(b). You can see that for each of the six symmetries of the base, the corresponding transformation, applied to the whole tetrahedron, results in the tetrahedron occupying the same space. Hence there are six ways of replacing the tetrahedron, or the reflected tetrahedron, on the base. Since there were four ways to choose the base, it follows that there are $4 \times 6 = 24$ symmetries of the tetrahedron.

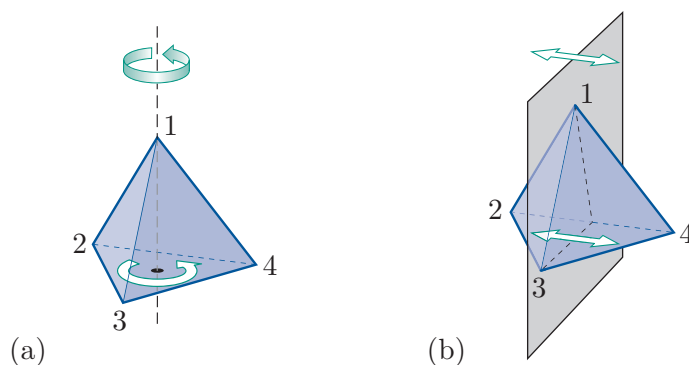


Figure 63 (a) Rotating the base and tetrahedron (b) Reflecting the base and tetrahedron

An argument similar to the one above holds for any regular polyhedron. In particular, once we have chosen a particular face to be the base, then for each symmetry of the base, the corresponding transformation applied to the whole polyhedron results in the polyhedron occupying the same space. It follows that the total number of symmetries of a regular polyhedron is the number of faces multiplied by the number of symmetries of each face. So we have the following strategy.

Strategy B1

To determine the number of symmetries of a regular polyhedron, do the following.

1. Count the number of faces.
2. Count the number of symmetries of a face.
3. Then

$$\left(\begin{array}{c} \text{number of} \\ \text{symmetries of the} \\ \text{regular polyhedron} \end{array} \right) = \left(\begin{array}{c} \text{number of} \\ \text{faces} \end{array} \right) \times \left(\begin{array}{c} \text{number of} \\ \text{symmetries of a face} \end{array} \right).$$

Exercise B31

Use Strategy B1 to show that the cube and the octahedron each have 48 symmetries, and that the dodecahedron and the icosahedron each have 120 symmetries.

(Remember that a regular n -gon has $2n$ symmetries, as described at the end of Subsection 1.1.)

Counting the symmetries of a non-regular polyhedron

Strategy B1 for determining the number of symmetries of a regular polyhedron can be adapted to allow us to find the number of symmetries of a non-regular polyhedron. To illustrate the method, let us consider two particular non-regular polyhedra.

First, we will look at the *pentagonal prism* shown in Figure 64, in which the top and bottom faces are regular pentagons, and the vertical faces are squares. (In general, a **prism** is a polyhedron two of whose faces are congruent, parallel polygons, and each of whose other faces is a parallelogram.)

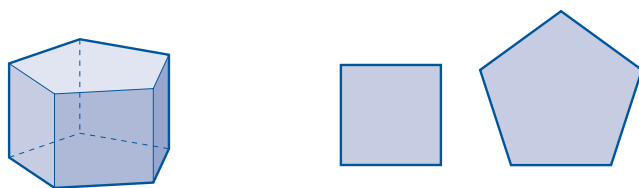


Figure 64 A pentagonal prism with square side faces, and its two face types

The pentagonal prism in Figure 64 has direct symmetries – for example, rotations about the vertical line through its centre, as shown in Figure 65(a). It also has indirect symmetries – for example, a reflection in a plane that contains a vertical edge of the prism and bisects the square face opposite this edge, as shown in Figure 65(b).

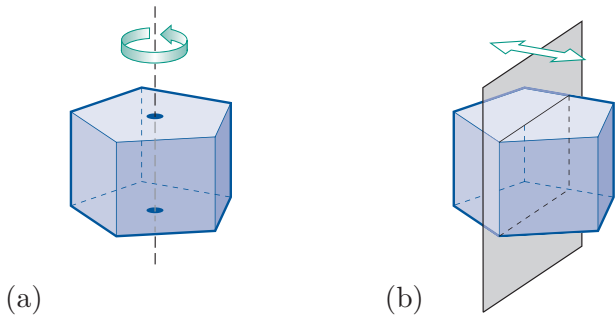


Figure 65 Rotational and reflectional symmetries of the pentagonal prism

To find the number of symmetries of the prism, we can count the number of ways of replacing the prism, or the reflected prism, in the space that it occupied originally, but possibly with the vertices at new locations.

In Figure 64, the prism is shown with a pentagonal face as its base, so we can choose either of the two pentagonal faces to be the base. The base has 10 symmetries, and we need to check whether, for each of these symmetries of the base, the corresponding transformation applied to the whole prism results in the prism occupying the same space. In other words, we need to check whether each of the 10 symmetries of the base gives a symmetry of the whole prism. You can see that this is indeed the case. So, for each of the two choices of base, there are 10 ways of replacing the prism, or the reflected prism, on the base. Thus there are $2 \times 10 = 20$ symmetries of the prism.

We carried out this calculation by considering one of the pentagonal faces as the base. We can check our answer by considering one of the square faces to be the base, as shown in Figure 66. This figure also indicates the shapes of the faces that share an edge with the square base.



Figure 66 The prism with a square face as the base

Again we count the number of ways of replacing the prism, or the reflected prism, in the space that it originally occupied. We can choose any of the five square faces to be the base.

We now have to be careful because only some of the eight symmetries of the square base give symmetries of the whole prism. For example, one

symmetry of the square base is a rotation of $\pi/2$ about its centre, but if we apply the corresponding transformation to the prism as a whole – that is, if we rotate the prism through $\pi/2$ about the vertical line through the centre of the square base, as shown in Figure 67 – then the prism does not occupy its original space in \mathbb{R}^3 . So this transformation is not a symmetry of the prism. One way to see this is to observe that a symmetry of the square base that maps an edge joined to a pentagonal face to an edge joined to a square face cannot give a symmetry of the whole prism. Similarly, reflections through the diagonals of the square base do not give symmetries of the prism.

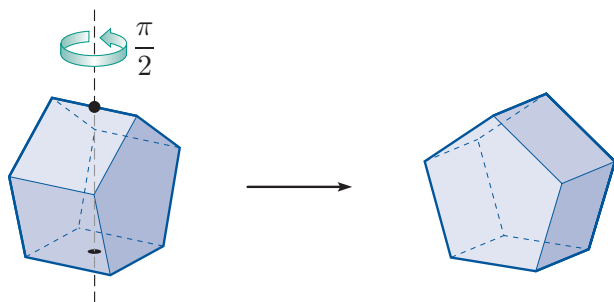


Figure 67 Rotation of the prism through $\pi/2$ about the vertical axis of symmetry

In fact, only four of the eight symmetries of the square base give symmetries of the prism, namely the identity, the rotation through π and the reflections in the lines joining the midpoints of opposite edges. Thus, since we can choose any of the five square faces to be the base, the number of symmetries of the prism is $5 \times 4 = 20$. This confirms our earlier answer.

Small rhombicuboctahedron

As a second example, we consider the polyhedron shown in Figure 68. It is called the **small rhombicuboctahedron**, and it has 18 square faces and 8 faces that are equilateral triangles. (It is not to be confused with the *great rhombicuboctahedron*, which has 12 square faces, 8 hexagonal faces and 6 octagonal faces.)

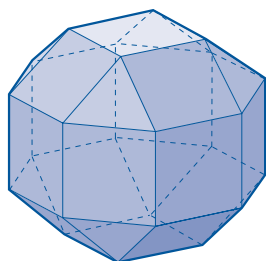


Figure 68 The small rhombicuboctahedron

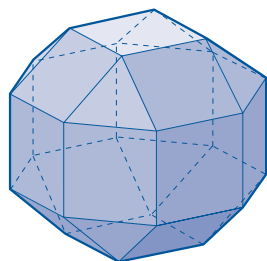


Figure 69 The small rhombicuboctahedron

To find the number of symmetries of the small rhombicuboctahedron, we can count the number of ways of replacing the polyhedron, or the reflected polyhedron, in the space that it occupied originally, as shown in Figure 69 with a square face as its base, but possibly with the vertices at new locations.

We immediately come across a new complication: only some of the square faces of the polyhedron can be placed as the base if the polyhedron, or its reflection, is to occupy its original space in \mathbb{R}^3 . This is because there are two types of square face in the small rhombicuboctahedron. For one type, all four edges of the face are joined to other square faces, whereas for the other type, two edges are joined to square faces and two to triangular faces, as shown in Figure 70.

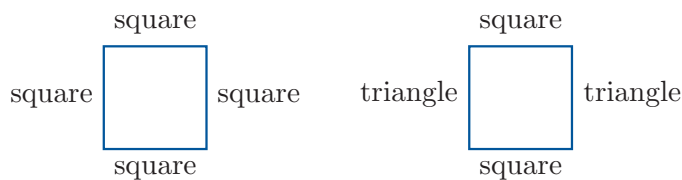


Figure 70 The two types of square face in the small rhombicuboctahedron

The small rhombicuboctahedron shown in Figure 69 has a square face of the first type as its base. There are six faces of this type in the polyhedron, and we can choose any of these to be placed as the base.

Next we have to determine how many of the eight symmetries of one of these square faces give symmetries of the polyhedron. Consideration of the polyhedron shows that all eight symmetries do, so the number of symmetries of the polyhedron is $6 \times 8 = 48$.

We could check this answer by taking one of the square faces of the second type, or one of the triangular faces, to be the base. In each case, we have to consider carefully how many symmetries of the base are symmetries of the whole polyhedron.

The two examples of counting the symmetries of a non-regular polyhedron that you have seen demonstrate the following general strategy.

Strategy B2

To determine the number of symmetries of a non-regular polyhedron, do the following.

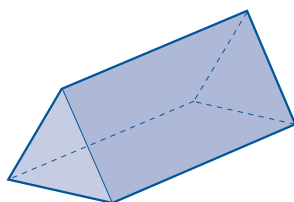
1. Select one type of face.
(For two faces to be of the same type, it must be possible to place the polyhedron with either of the faces as its base and have it occupy the same space.)
2. Count the number of faces of this type.
3. Count the symmetries of a face of this type that give symmetries of the polyhedron.

4. Then

$$\left(\begin{array}{c} \text{number of} \\ \text{symmetries of} \\ \text{the polyhedron} \end{array} \right) = \left(\begin{array}{c} \text{number of} \\ \text{faces of the} \\ \text{selected type} \end{array} \right) \times \left(\begin{array}{c} \text{number of} \\ \text{symmetries of a face} \\ \text{of this type that} \\ \text{give symmetries of} \\ \text{the polyhedron} \end{array} \right).$$

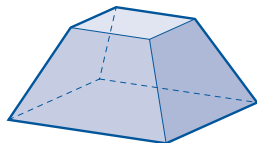
Exercise B32

Using Strategy B2, determine the number of symmetries of the triangular prism shown below. It has two faces that are equilateral triangles, and three faces that are non-square rectangles. Check your calculation by considering the solid in a different way.



Exercise B33

Determine the number of symmetries of the solid shown below, which has two square faces of different sizes, and four faces that are trapeziums with two equal edges.



In fact the symmetries of the solid in Exercise B33 are just the symmetries given by the eight symmetries of its square base, and hence it has eight symmetries. There are many solids whose symmetries are just the symmetries given by a related plane figure. For example, the symmetries of the hexagonal bottle in Figure 71 are the symmetries given by its hexagonal base, and hence it has 12 symmetries.

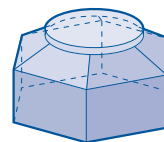


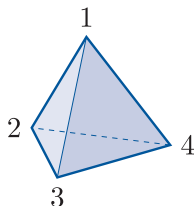
Figure 71 A hexagonal bottle

5.3 Finding the symmetries of a polyhedron

In this subsection you will see an example of how to actually find the symmetries of a polyhedron, once we know how many there are. The approach that we will take here allows us to describe the symmetries geometrically, as far as possible, as well as find their two-line symbols.

Worked Exercise B14

Find all the symmetries of the regular tetrahedron, shown below, describing them geometrically.



Solution

By Strategy B1, the tetrahedron has $4 \times 6 = 24$ symmetries (as found in the previous subsection). Since it has at least one indirect symmetry (such as reflection in the vertical plane that contains the edge joining locations 1 and 3), it has 12 direct symmetries and 12 indirect symmetries.

First we find the direct symmetries.

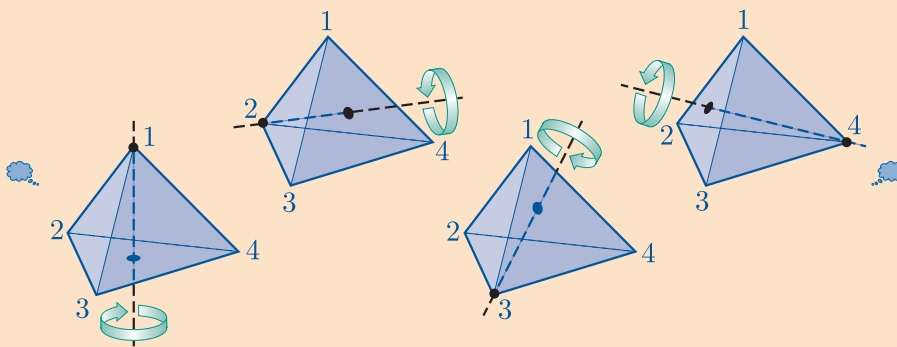
We always have the identity symmetry.

One direct symmetry is the identity symmetry,

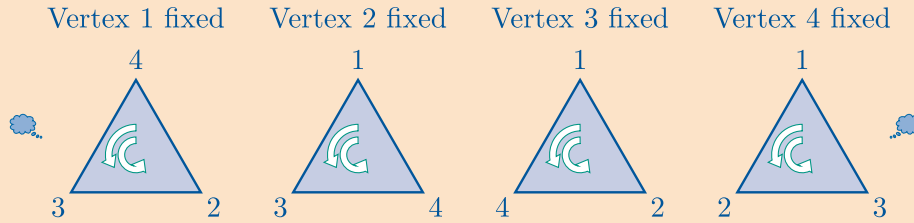
$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Look for non-trivial rotational symmetries.

For each vertex, there is an axis of symmetry that passes through the vertex and the centre of the opposite face.



A rotational symmetry about such an axis fixes the vertex that lies on the axis and rotates the opposite face.



There are two non-trivial rotational symmetries about each such axis, as follows.

The axis through the vertex at location 1 gives the rotations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

The axis through the vertex at location 2 gives the rotations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

The axis through the vertex at location 3 gives the rotations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

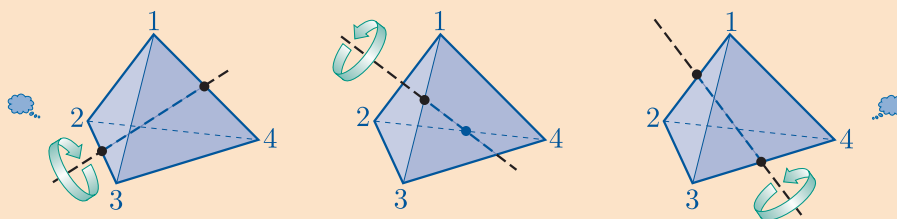
The axis through the vertex at location 4 gives the rotations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

☁ We have now found nine direct symmetries, so there are three more. If we cannot spot them immediately, then we can try composing some of the direct symmetries found already, since a composite of direct symmetries is a direct symmetry. Composing the first and fourth non-trivial direct symmetries above gives

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

This is a new direct symmetry. It interchanges the vertices at locations 1 and 4 and interchanges the vertices at locations 2 and 3. Geometrically, it is a rotation through π about the line through the midpoints of the opposite edges joining 1 to 4 and 2 to 3. There is a similar rotational symmetry for each of the other two pairs of opposite edges. ☁

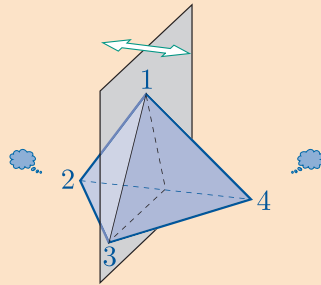


There are three rotations through axes of symmetry that join midpoints of opposite edges, as follows:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

We have now found all 12 direct symmetries of the tetrahedron.

To find the indirect symmetries, find one reflectional symmetry, and compose it with all the direct symmetries already found (being consistent about whether the indirect symmetry is composed on the right or the left). An example of a reflectional symmetry is shown below.



One reflectional symmetry is reflection in the vertical plane through the edge joining the vertices at locations 1 and 3 and the midpoint of the edge joining the vertices at locations 2 and 4, that is,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Composing each of the 12 direct symmetries with this indirect symmetry on the right gives the following twelve indirect symmetries.

$$\begin{array}{cccc} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \end{array}$$

Six of these indirect symmetries (the ones that fix two vertices and interchange two vertices) are reflections in a plane that passes through an edge and the midpoint of the opposite edge. There is one such reflectional symmetry for each of the six edges of the tetrahedron.

The remaining six indirect symmetries are not reflections, because the effect of a reflection on a point is to fix it (if it lies on the plane of reflection) or interchange it with another point (if it does not), and these six symmetries do not have that effect on the vertices. For

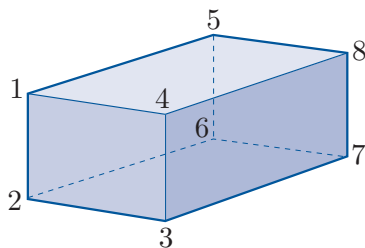
example, the fourth indirect symmetry above maps the vertex at location 1 to the vertex at location 3, but it does not map the vertex at location 3 to the vertex at location 1. ☁

The other six indirect symmetries do not have a simple geometric description: each of them is the composite of a reflection and a rotation.

In the worked exercise above it was mentioned that if a symmetry f is a reflection, then each point is either fixed by f or interchanged by f with another point. Note that the converse of this fact is not true: that is, a symmetry may have this effect on all points, but not be a reflection. For example, a rotation through π has this effect, as you will see in the next exercise.

Exercise B34

- (a) Use Strategy B2 to show that the cuboid shown below has eight symmetries. Each of its faces is a non-square rectangle.



- (b) Write down the two-line symbol for each of the eight symmetries, using the location labelling shown above.

You have seen that the set of symmetries of any figure in two- or three-dimensional space is a group under function composition. So, in particular, the 24 symmetries of the tetrahedron found in Worked Exercise B14 form a group under function composition, as do the eight symmetries of the cuboid found in Exercise B34. If we wished, we could construct the Cayley table for either of these groups by composing the elements using the two-line symbols for the symmetries. (For the tetrahedron, this would take rather a long time, and yield rather a large table!)

5.4 The Platonic solids

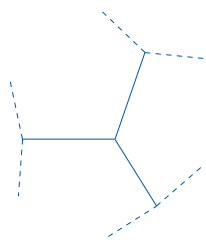


Figure 72 Three faces meeting at a vertex

As you saw in Subsection 5.1, the Platonic solids are the convex polyhedra in which all the faces are congruent regular polygons and at each vertex the same number of faces meet, arranged in the same way. If you are interested in understanding why there are only five such solids, then read the explanation below. This material will not be assessed.

Consider a solid of the description above. As for any solid, it must have at least three faces meeting at each vertex, as shown in Figure 72.

First suppose that the faces of the solid are equilateral triangles. There could be three, four or five equilateral triangles meeting at each vertex, as shown in Figure 73, but no more, as six equilateral triangles would lie flat, and more than six equilateral triangles would give a non-convex solid.

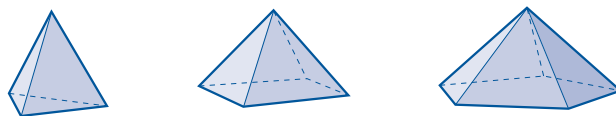


Figure 73 Three, four or five equilateral triangle faces meeting at a vertex

The arrangement of faces at each vertex of the solid must be the same, so we can build up the rest of the solid from the arrangement at one vertex. The three possibilities in Figure 73 give the tetrahedron, the octahedron and the icosahedron, respectively, as shown in Figure 74.

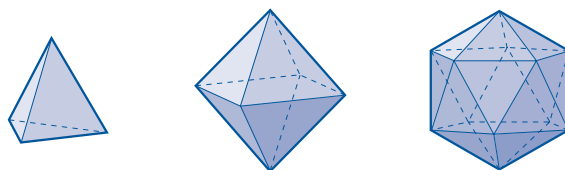


Figure 74 The regular tetrahedron, octahedron and icosahedron

Now suppose that the faces are not equilateral triangles, but squares. Three squares meeting at each vertex gives a cube. There cannot be more than three squares meeting at each vertex, because four squares would lie flat, and more than four squares would give a non-convex solid.

Next, suppose that the faces are regular pentagons. Three pentagons meeting at each vertex gives a dodecahedron. There cannot be more than three pentagons meeting at each vertex, as that would give a non-convex solid.

The cube and dodecahedron are shown in Figure 75.

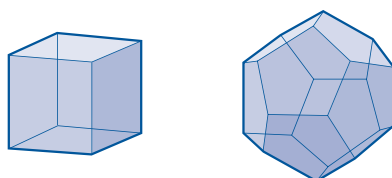


Figure 75 The cube and regular dodecahedron

There can be no more such solids, because three regular hexagons lie flat, and for any regular polygon with more than six edges, the angle at each vertex is greater than $2\pi/3$, so we cannot fit three together at a vertex without making the solid non-convex. (The angle at a vertex of a regular n -gon is $\pi - (2\pi/n)$, as shown in Figure 76, which is greater than $2\pi/3$ for $n > 6$.)

Thus there are precisely five regular polyhedra.

The Greek mathematician Theaetetus (c.417–c.368 BCE) may have been the first to recognise that there are only five regular solids, and only a few years later Plato incorporated a discussion of Theaetetus' work in his own *Timaeus*. Book XIII of Euclid's *Elements* (c.300 BCE), which completely describes the regular solids, contains a proof that there are only five of them.

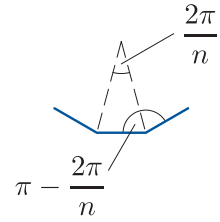


Figure 76 Angles in a regular n -gon

Summary

In this unit, you studied the symmetries of bounded figures in \mathbb{R}^2 and \mathbb{R}^3 , and saw that composition of symmetries is closed and associative, that there is an identity symmetry and that every symmetry has an inverse. You saw that these properties are the group axioms, which are satisfied by other binary operations on sets in many areas of mathematics. Such a set with its binary operation is called a group, and if the binary operation is also commutative, the group is called abelian. You practised checking whether the group axioms hold, and met many examples of groups, including groups, both infinite and finite, whose elements are numbers and whose binary operation is addition, multiplication, modular addition or modular multiplication. You saw how to use the group axioms to deduce further properties that apply to all groups. For example, the identity and inverses in a group are unique, and the left and right cancellation laws always hold. In the remaining units in this book, you will see that we can say a great deal more about the structure of groups by making further deductions from the group axioms.

Learning outcomes

After working through this unit, you should be able to:

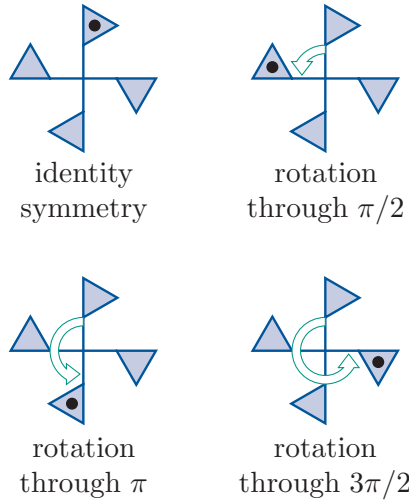
- explain what is meant by a *symmetry* of a figure in \mathbb{R}^2 or \mathbb{R}^3
- understand the difference between *direct* and *indirect* symmetries in \mathbb{R}^2 and \mathbb{R}^3
- find the symmetries of some bounded figures in \mathbb{R}^2 or \mathbb{R}^3 as *two-line symbols*, and describe them geometrically
- use two-line symbols to compose and invert symmetries
- explain the meaning of the terms *group*, *abelian* group and the *order* of a group
- determine whether a given set and *binary operation* form a group, by checking the group axioms
- construct a *Cayley table* for a finite set and binary operation, and use it to help you check the group axioms
- deduce information about a group from a *group table*
- be familiar with some standard types of groups, such as the groups formed by the symmetries of figures under function composition, groups of numbers under addition and multiplication, and groups from modular arithmetic
- know some basic properties of groups, such as that the identity in a group is unique and each element in a group has a unique inverse
- start to appreciate how some simple group properties can be proved by using the group axioms.

Solutions to exercises

Solution to Exercise B1

(a) We can denote the initial position by a dot at the top.

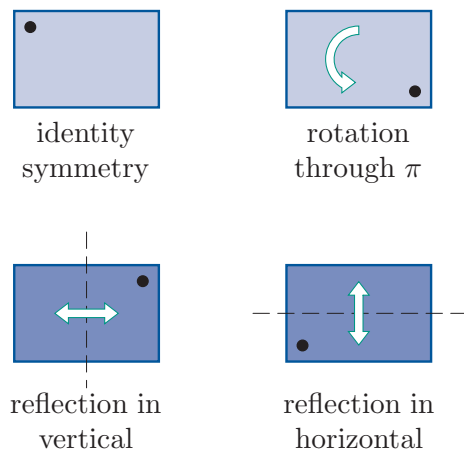
The symmetries are as follows.



(There are no reflectional symmetries.)

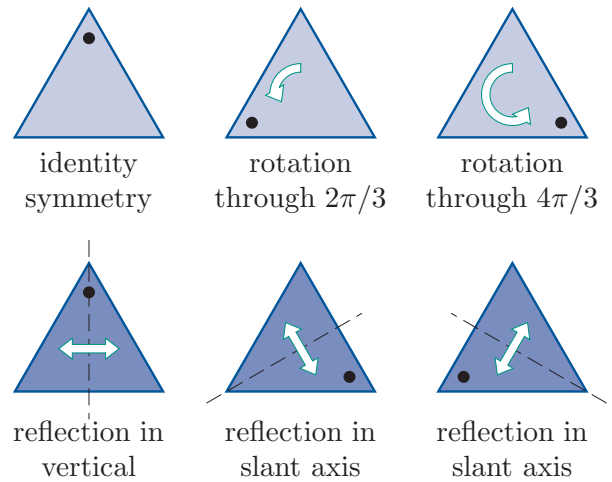
(b) We can denote the initial position by a light colour and a dot in the top left corner, and think of a darker colour on the 'reverse'.

The symmetries are as follows.



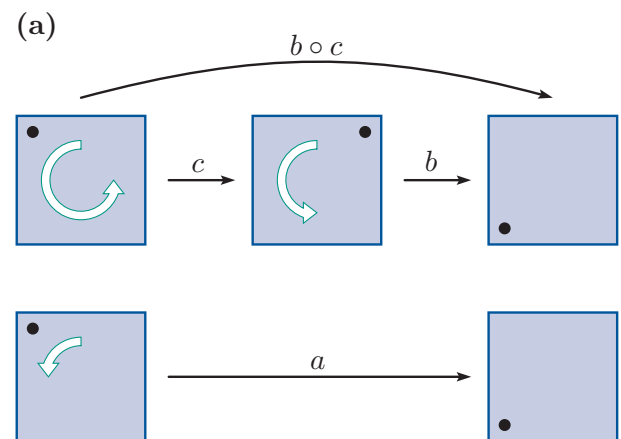
(c) We can denote the initial position by a light colour and a dot in the top corner, and think of a darker colour on the 'reverse'.

The symmetries are as follows.

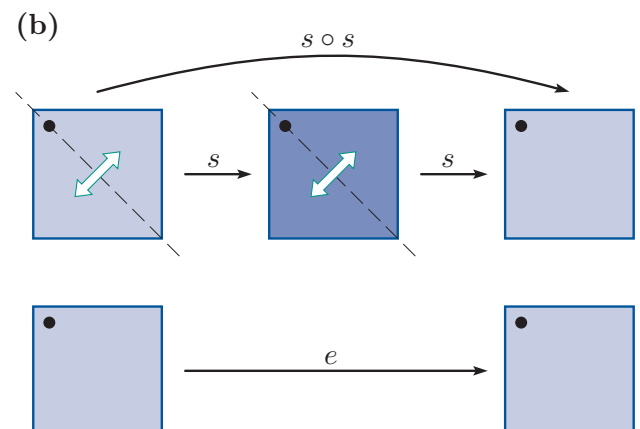


Solution to Exercise B2

We find the required composites by drawing diagrams similar to those in Worked exercise B1.

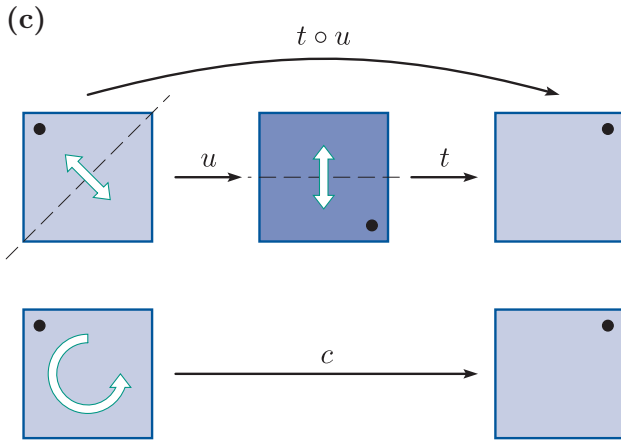


Hence $b \circ c = a$.



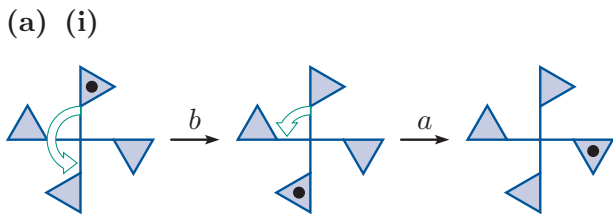
Hence $s \circ s = e$.

(Any reflection composed with itself is the same as the identity symmetry e .)

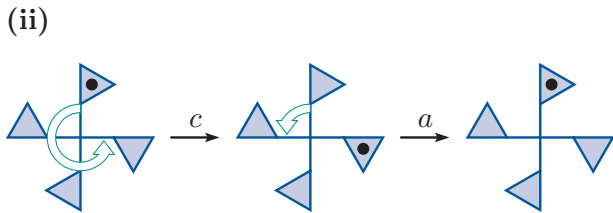


Hence $t \circ u = c$.

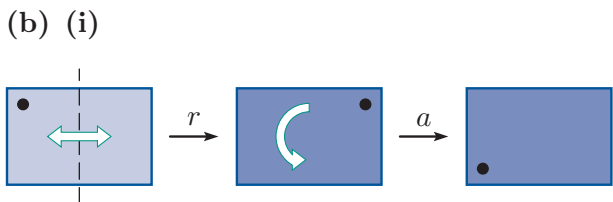
Solution to Exercise B3



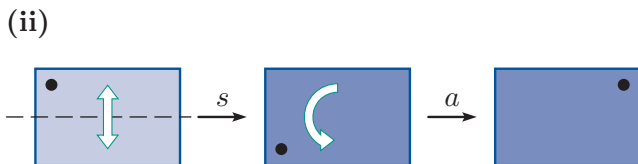
Hence $a \circ b = c$.



Hence $a \circ c = e$.

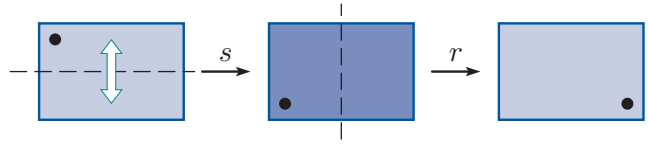


Hence $a \circ r = s$.



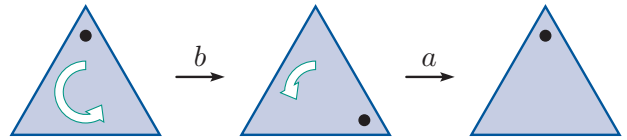
Hence $a \circ s = r$.

(iii)



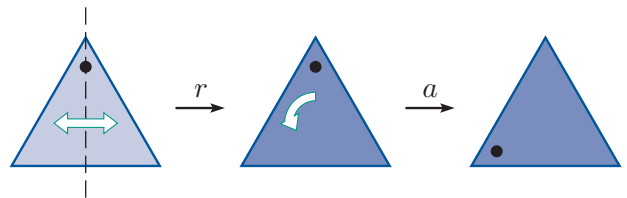
Hence $r \circ s = a$.

(c) (i)



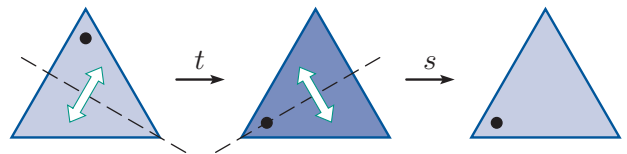
Hence $a \circ b = e$.

(ii)



Hence $a \circ r = t$.

(iii)



Hence $s \circ t = a$.

Solution to Exercise B4

We find the composites using the diagrammatic method demonstrated in Worked Exercise B1. (The diagrams are not given here.)

First we find $a \circ (t \circ a)$:

$$t \circ a = s \quad \text{and} \quad a \circ s = t,$$

so $a \circ (t \circ a) = t$.

Next we find $(a \circ t) \circ a$:

$$a \circ t = u \quad \text{and} \quad u \circ a = t,$$

so $(a \circ t) \circ a = t$.

Hence

$$a \circ (t \circ a) = (a \circ t) \circ a.$$

Solution to Exercise B5

(a) In $S(\triangle)$, as in $S(\square)$, the rotations a and c are inverses of each other, and b is self-inverse.

Element	e	a	b	c
Inverse	e	c	b	a

(b) In $S(\square)$, each element is self-inverse.

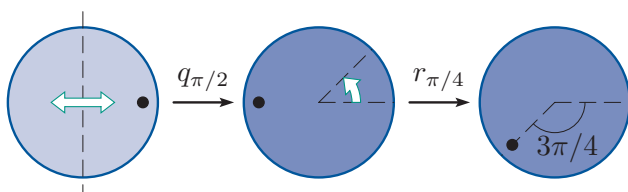
Element	e	a	r	s
Inverse	e	a	r	s

(c) In $S(\triangle)$, the rotations a and b are inverses of each other, and the other symmetries are self-inverse.

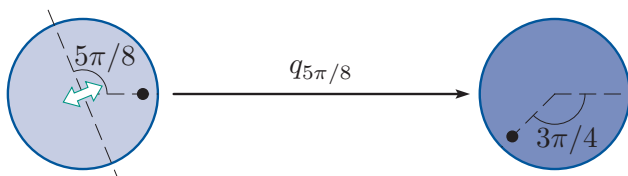
Element	e	a	b	r	s	t
Inverse	e	b	a	r	s	t

Solution to Exercise B6

We find $r_{\pi/4} \circ q_{\pi/2}$ using the following diagram.



Hence $r_{\pi/4} \circ q_{\pi/2} = q_{5\pi/8}$, as shown below.

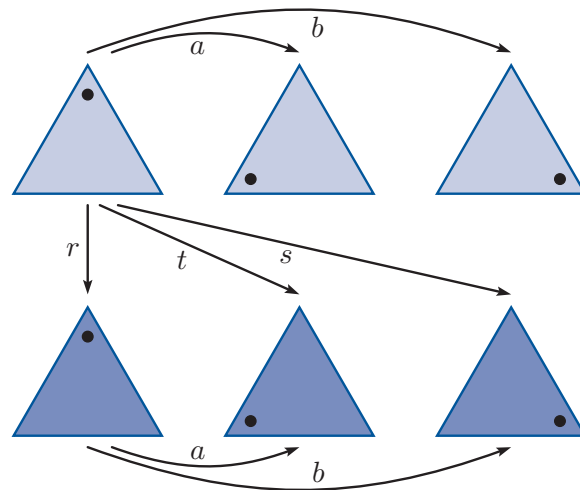


Solution to Exercise B7

(a) The set of direct symmetries of the equilateral triangle is

$$S^+(\triangle) = \{e, a, b\}.$$

Using the reflection r , we obtain the following diagram.



$$r = e \circ r \quad t = a \circ r \quad s = b \circ r$$

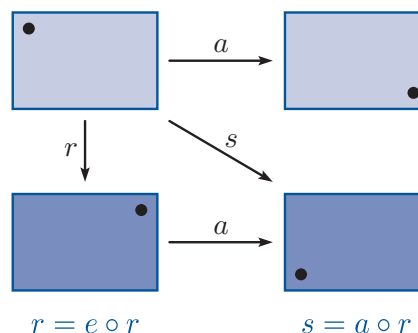
Instead of r , we could have used s or t as the reflection:

$$\begin{aligned} s &= e \circ s, & r &= a \circ s, & t &= b \circ s, \\ t &= e \circ t, & s &= a \circ t, & r &= b \circ t. \end{aligned}$$

(b) The set of direct symmetries of the rectangle is

$$S^+(\square) = \{e, a\}.$$

Using the reflection r , we obtain the following diagram.



$$r = e \circ r$$

$$s = a \circ r$$

Alternatively, we could have used the reflection s :

$$s = e \circ s, \quad r = a \circ s.$$

Solution to Exercise B8

We have

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad u = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Solution to Exercise B9

Here

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

(Remember to include e .)

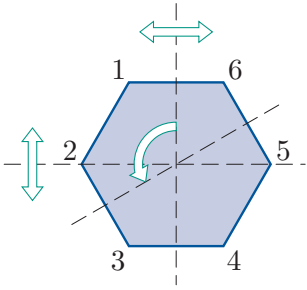
Solution to Exercise B10

We have

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Solution to Exercise B11



(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ represents reflection in the vertical axis of symmetry.

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ represents anticlockwise rotation through $2\pi/3$ about the centre.

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}$ represents reflection in the horizontal axis of symmetry.

Solution to Exercise B12

We have

$$a \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = b,$$

$$b \circ s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = t,$$

$$s \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = r,$$

$$t \circ s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = b.$$

Solution to Exercise B13

In each case we turn the two-line symbol upside down and reorder the columns.

$$(a) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 5 & 6 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 1 & 6 & 5 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$$

$$(c) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 5 & 6 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

Solution to Exercise B14

We have

$$b \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = a,$$

$$b \circ t = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = r,$$

$$t \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s,$$

$$t \circ t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$$

Thus the Cayley table for $S(\triangle)$ is as follows.

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

Solution to Exercise B15

The symmetry a is a half-turn, so $a \circ a = e$.

The symmetry s is a reflection, so $s \circ s = e$.

Also,

$$\begin{aligned} a \circ s &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = r, \end{aligned}$$

and

$$\begin{aligned} s \circ a &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = r. \end{aligned}$$

Thus the Cayley table for $S(\square)$ is as follows.

\circ	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

Solution to Exercise B16

(a) We check the group axioms for $(\mathbb{Z}, +)$. The arguments are similar to those in Worked Exercise B7.

G1 For all $m, n \in \mathbb{Z}$,

$$m + n \in \mathbb{Z},$$

since the sum of two integers is an integer. So \mathbb{Z} is closed under addition.

G2 Addition of integers is associative.

G3 We have $0 \in \mathbb{Z}$, and for all $n \in \mathbb{Z}$,

$$n + 0 = n = 0 + n.$$

So 0 is an identity element for addition on \mathbb{Z} .

G4 For each $n \in \mathbb{Z}$, we have $-n \in \mathbb{Z}$, and

$$n + (-n) = 0 = (-n) + n,$$

so $-n$ is an inverse of n .

Thus each element of \mathbb{Z} has an inverse in \mathbb{Z} with respect to addition.

Hence $(\mathbb{Z}, +)$ satisfies the four group axioms, and so is a group.

(b) We check the group axioms for (\mathbb{Q}^*, \times) . The arguments are similar to those in Worked Exercise B8.

G1 Let $x, y \in \mathbb{Q}^*$. Then $x \times y \in \mathbb{Q}$, since the product of two rational numbers is a rational number. Also $x \times y \neq 0$, since $x \neq 0$ and $y \neq 0$. Hence

$$x \times y \in \mathbb{Q}^*,$$

so \mathbb{Q}^* is closed under multiplication.

G2 Multiplication of rational numbers is associative.

G3 We have $1 \in \mathbb{Q}^*$, and for all $x \in \mathbb{Q}^*$,

$$x \times 1 = x = 1 \times x.$$

So 1 is an identity element for multiplication on \mathbb{Q}^* .

G4 Let $x \in \mathbb{Q}^*$. Then $x \neq 0$, so $1/x$ exists, and lies in \mathbb{Q}^* , since the reciprocal of a non-zero rational number is a non-zero rational number. Also

$$x \times \frac{1}{x} = 1 = \frac{1}{x} \times x.$$

Hence $1/x$ is an inverse of x .

Thus each element of \mathbb{Q}^* has an inverse in \mathbb{Q}^* with respect to multiplication.

Hence (\mathbb{Q}^*, \times) satisfies the four group axioms, and so is a group.

Solution to Exercise B17

(a) The set \mathbb{Q} is closed under multiplication; multiplication of rational numbers is associative; and 1 is a multiplicative identity in \mathbb{Q} , so axioms G1, G2 and G3 hold.

However, axiom G4 fails, because 0 has no multiplicative inverse in \mathbb{Q} .

Hence (\mathbb{Q}, \times) is not a group.

(b) The sum of two positive real numbers is a positive real number, so \mathbb{R}^+ is closed under addition. Also, addition of real numbers is associative. So axioms G1 and G2 hold.

However, axiom G3 fails: there is no identity element. This is because, for example, there is no element $e \in \mathbb{R}^+$ such that

$$2 + e = 2,$$

since $0 \notin \mathbb{R}^+$.

Hence $(\mathbb{R}^+, +)$ is not a group.

(c) The product of two odd integers is odd, so D is closed under multiplication. Multiplication of integers is associative. Also, 1 is odd, so 1 is a multiplicative identity in D . So axioms G1, G2 and G3 hold.

However, axiom G4 fails because, for example, 3 has no multiplicative inverse in D , since $\frac{1}{3} \notin D$.

Hence (D, \times) is not a group.

(d) We show that the four group axioms hold.

G1 If m and n are even numbers, then $m + n$ is an even number, so E is closed under $+$.

G2 Addition of numbers is associative.

G3 We have $0 \in E$ (since 0 is even), and for all $n \in E$,

$$n + 0 = n = 0 + n,$$

so 0 is an identity element for $+$ on E .

G4 For each even number n , the number $-n$ is also even, and

$$n + (-n) = 0 = (-n) + n,$$

so $-n$ is an inverse of n .

Hence $(E, +)$ satisfies the four group axioms, and so is a group.

(e) The set E is closed under subtraction, so axiom G1 holds.

However, axiom G2 (associativity) fails. For example, the numbers 6, 4 and 2 belong to E , and

$$6 - (4 - 2) = 6 - 2 = 4,$$

but

$$(6 - 4) - 2 = 2 - 2 = 0.$$

Since $4 \neq 0$, subtraction is not associative on E .

Hence $(E, -)$ is not a group.

Alternatively, we can show that axiom G3 (identity) fails. There is no identity element, since, for example, there is no even integer n such that

$$2 - n = 2 = n - 2.$$

(f) The numbers -1 and -2 lie in M , but

$$(-1) \times (-2) = 2 \notin M.$$

So M is not closed under \times . That is, axiom G1 fails.

Solution to Exercise B18

The approach is similar to that in Worked Exercise B11.

An identity element $e \in \mathbb{R}$ must have the property that, for each $x \in \mathbb{R}$,

$$x \circ e = x = e \circ x.$$

The equation $x \circ e = x$ gives

$$x - e - 1 = x,$$

which gives

$$e = -1.$$

So the only possibility for an identity element is $e = -1$.

However, if $e = -1$, then

$$e \circ x = -1 \circ x = -1 - x - 1 = -2 - x,$$

and $-2 - x$ is not equal to x in general, because, for example, taking $x = 0$ gives $-2 - x = -2 \neq 0$.

So -1 is not an identity element for (\mathbb{R}, \circ) , and hence there is no identity element.

That is, axiom G3 fails.

Hence (\mathbb{R}, \circ) is not a group.

(Note that axiom G2 (associativity) also fails for the set \mathbb{R} with this binary operation.)

Solution to Exercise B19

(a) Let $x, y, z \in \mathbb{R}$. Then

$$\begin{aligned} x \circ (y \circ z) &= x \circ (y + z - yz) \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - xy - xz - yz + xyz \end{aligned}$$

and

$$\begin{aligned} (x \circ y) \circ z &= (x + y - xy) \circ z \\ &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y + z - xy - xz - yz + xyz. \end{aligned}$$

The two expressions obtained are the same, so \circ is associative on \mathbb{R} .

(b) Let $x, y, z \in \mathbb{R}$. Then

$$\begin{aligned} x \circ (y \circ z) &= x \circ (y - z + yz) \\ &= x - (y - z + yz) + x(y - z + yz) \\ &= x - y + z + xy - xz - yz + xyz \end{aligned}$$

and

$$\begin{aligned} (x \circ y) \circ z &= (x - y + xy) \circ z \\ &= (x - y + xy) - z + (x - y + xy)z \\ &= x - y - z + xy + xz - yz + xyz. \end{aligned}$$

The two expressions obtained are not equivalent.

For example, if $x = 0$, $y = 1$ and $z = 2$, then

$$\begin{aligned} 0 \circ (1 \circ 2) &= 0 \circ (1 - 2 + 2) \\ &= 0 \circ 1 \\ &= 0 - 1 + 0 = -1 \end{aligned}$$

but

$$\begin{aligned} (0 \circ 1) \circ 2 &= (0 - 1 + 0) \circ 2 \\ &= (-1) \circ 2 \\ &= -1 - 2 - 2 = -5. \end{aligned}$$

So \circ is not associative.

(If you can see that a binary operation \circ is not associative, then you do not need to find the general expressions for $x \circ (y \circ z)$ and $(x \circ y) \circ z$. It is enough to give a specific counterexample to demonstrate that \circ is not associative.)

Solution to Exercise B20

We show that the four group axioms hold.

G1 For all $a, b \in \mathbb{Q}^+$, we have $a \circ b = \frac{1}{2}ab \in \mathbb{Q}^+$, so \mathbb{Q}^+ is closed under \circ .

G2 For all $a, b, c \in \mathbb{Q}^+$,

$$\begin{aligned} a \circ (b \circ c) &= a \circ \left(\frac{1}{2}bc\right) \\ &= \frac{1}{2}a\left(\frac{1}{2}bc\right) \\ &= \frac{1}{4}abc \end{aligned}$$

and

$$\begin{aligned} (a \circ b) \circ c &= \left(\frac{1}{2}ab\right) \circ c \\ &= \frac{1}{2}\left(\frac{1}{2}ab\right)c \\ &= \frac{1}{4}abc. \end{aligned}$$

The two expressions obtained are the same, so \circ is associative on \mathbb{Q}^+ .

G3 We try to find a likely candidate for the

identity. We seek an element $e \in \mathbb{Q}^+$ such that, for all $a \in \mathbb{Q}^+$,

$$a \circ e = a = e \circ a.$$

The equation $a \circ e = a$ gives

$$\frac{1}{2}ae = a,$$

which gives $e = 2$.

Now $2 \in \mathbb{Q}^+$, and for all $a \in \mathbb{Q}^+$,

$$a \circ 2 = \frac{1}{2} \times a \times 2 = a$$

and

$$2 \circ a = \frac{1}{2} \times 2 \times a = a.$$

So 2 is indeed an identity element for (\mathbb{Q}^+, \circ) .

G4 Let $a \in \mathbb{Q}^+$. An inverse of a is not obvious, so we try to find a likely candidate. We seek an element $x \in \mathbb{Q}^+$ such that

$$a \circ x = 2 = x \circ a.$$

The equation $a \circ x = 2$ gives $\frac{1}{2}ax = 2$ and hence $x = 4/a$, so the only possibility for an inverse of a is $4/a$.

Now $4/a \in \mathbb{Q}^+$, and

$$a \circ \frac{4}{a} = \frac{1}{2} \times a \times \frac{4}{a} = 2$$

and

$$\frac{4}{a} \circ a = \frac{1}{2} \times \frac{4}{a} \times a = 2.$$

So $4/a$ is an inverse of a .

Hence (\mathbb{Q}^+, \circ) satisfies the four group axioms, and so is a group.

Solution to Exercise B21

(a) This situation is similar to that in Worked Exercise B12.

The Cayley table for $(\mathbb{Z}_5, +_5)$ is as follows.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

We show that the four group axioms hold.

G1 All the elements in the table are in \mathbb{Z}_5 , so \mathbb{Z}_5 is closed under $+_5$.

G2 The operation $+_5$ is associative.

G3 The row and column labelled 0 repeat the table borders, so 0 is an identity element.

G4 From the Cayley table, we see that

$$\begin{aligned} 0 +_5 0 &= 0, \\ 1 +_5 4 &= 0 = 4 +_5 1, \\ 2 +_5 3 &= 0 = 3 +_5 2, \end{aligned}$$

so

$$\begin{aligned} 0 &\text{ is self-inverse,} \\ 1 \text{ and } 4 &\text{ are inverses of each other,} \\ 2 \text{ and } 3 &\text{ are inverses of each other.} \end{aligned}$$

Hence $(\mathbb{Z}_5, +_5)$ satisfies the four group axioms, and so is a group.

(b) This situation is similar to that in Worked Exercise B13.

The Cayley table for (\mathbb{Z}_5, \times_5) is as follows.

\times_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Axioms G1, G2 and G3 hold, and 1 is an identity element.

However, there is no 1 in the row labelled 0, so 0 has no inverse and therefore axiom G4 fails.

Hence (\mathbb{Z}_5, \times_5) is not a group.

(c) In this case, the troublesome 0 in part (b) has been omitted, and the Cayley table is as follows.

\times_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We check the four group axioms in turn.

G1 All the elements in the table are in $\{1, 2, 3, 4\}$, so $\{1, 2, 3, 4\}$ is closed under \times_5 .

G2 The operation \times_5 is associative.

G3 The row and column labelled 1 repeat the table borders, so 1 is an identity element.

G4 From the table, we see that

$$\begin{aligned} 1 \times_5 1 &= 1, \\ 4 \times_5 4 &= 1, \\ 2 \times_5 3 &= 1 = 3 \times_5 2, \end{aligned}$$

so

$$\begin{aligned} 1 \text{ and } 4 &\text{ are self-inverse,} \\ 2 \text{ and } 3 &\text{ are inverses of each other.} \end{aligned}$$

Hence $(\{1, 2, 3, 4\}, \times_5)$ satisfies the four group axioms, and so is a group.

(d) The Cayley table for $(\{1, 2, 3, 4, 5\}, \times_6)$ is as follows.

\times_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

The body of the table contains occurrences of the number 0, which is not an element of $\{1, 2, 3, 4, 5\}$, so axiom G1 fails.

Hence $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group.

(Another way to show that $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group is to show that axiom G4 fails. The number 1 is an identity element for $(\{1, 2, 3, 4, 5\}, \times_6)$, but there is no 1 in the row labelled 2, so 2 has no inverse.)

(e) The Cayley table for $(\{2, 4, 6, 8\}, \times_{10})$ is as follows.

\times_{10}	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

We check the four group axioms in turn.

G1 All the elements in the table are in $\{2, 4, 6, 8\}$, so $\{2, 4, 6, 8\}$ is closed under \times_{10} .

G2 The operation \times_{10} is associative.

G3 The row and column labelled 6 repeat the table borders, so 6 is an identity element.

G4 From the table, we see that

$$\begin{aligned} 4 \times_{10} 4 &= 6, \\ 6 \times_{10} 6 &= 6, \\ 2 \times_{10} 8 &= 6 = 8 \times_{10} 2, \end{aligned}$$

so

4 and 6 are self-inverse,

2 and 8 are inverses of each other.

Hence $(\{2, 4, 6, 8\}, \times_{10})$ satisfies the four group axioms, and so is a group.

(f) The Cayley table for $(\{1, -1\}, \times)$ is as follows.

\times	1	-1
1	1	-1
-1	-1	1

We check the four group axioms in turn.

G1 All the elements in the table are in $\{1, -1\}$, so this set is closed under \times .

G2 Multiplication of numbers is associative.

G3 From the table, we see that 1 is an identity element.

G4 Since $1 \times 1 = 1$ and $(-1) \times (-1) = 1$, the elements 1 and -1 are both self-inverse.

Hence $(\{1, -1\}, \times)$ satisfies the four group axioms, and so is a group.

Solution to Exercise B22

We check the four group axioms in turn.

G1 All the elements in the table are in $\{a, b, c, d, e, f, g, h\}$, so this set is closed under \circ .

G2 We are told that the operation \circ is associative.

G3 The row and column labelled e repeat the table borders, so e is an identity element.

G4 From the table, we see that

$$a \circ b = e = b \circ a,$$

$$c \circ d = e = d \circ c,$$

$$e \circ e = e,$$

$$f \circ f = e,$$

$$g \circ h = e = h \circ g,$$

so

e and f are self-inverse,

a and b are inverses of each other,

c and d are inverses of each other,

g and h are inverses of each other.

Hence $(\{a, b, c, d, e, f, g, h\}, \circ)$ satisfies the four group axioms, and so is a group.

Solution to Exercise B23

(a) A Cayley table for $(\mathbb{Z}_7, +_7)$ is

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

The inverses of the elements are as follows.

Element	0	1	2	3	4	5	6
Inverse	0	6	5	4	3	2	1

(b) A Cayley table for $(\mathbb{Z}_7^*, \times_7)$ is

\times_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

The inverses of the elements are as follows.

Element	1	2	3	4	5	6
Inverse	1	4	5	2	3	6

(c) We have

$$U_{10} = \{1, 3, 7, 9\}.$$

A Cayley table for (U_{10}, \times_{10}) is

\times_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

The inverses of the elements are as follows.

Element	1	3	7	9
Inverse	1	7	3	9

(d) We have

$$U_9 = \{1, 2, 4, 5, 7, 8\}.$$

A Cayley table for (U_9, \times_9) is

\times_9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

The inverses of the elements are as follows.

Element	1	2	4	5	7	8
Inverse	1	5	7	2	4	8

Solution to Exercise B24

Suppose that, in a group (G, \circ) ,

$$a \circ x = b \circ x.$$

Composing both sides on the right with the inverse of x , we obtain

$$a \circ x \circ x^{-1} = b \circ x \circ x^{-1}.$$

By axiom G2 (associativity), this gives

$$a \circ (x \circ x^{-1}) = b \circ (x \circ x^{-1}).$$

Hence, by axiom G4 (inverses), we obtain

$$a \circ e = b \circ e,$$

and therefore, by axiom G3 (identity),

$$a = b.$$

Solution to Exercise B25

We know that

$$a \circ b \circ c = e.$$

Composing both sides on the left with the inverse of a gives

$$a^{-1} \circ a \circ b \circ c = a^{-1} \circ e.$$

By axiom G2 (associativity), this gives

$$(a^{-1} \circ a) \circ b \circ c = a^{-1} \circ e.$$

Hence, by axiom G4 (inverses), we obtain

$$e \circ b \circ c = a^{-1} \circ e,$$

and therefore, by axiom G3 (identity),

$$b \circ c = a^{-1}.$$

Now composing both sides on the right by a gives

$$b \circ c \circ a = a^{-1} \circ a.$$

Hence, by axiom G4 (inverses), we obtain

$$b \circ c \circ a = e,$$

as required.

Solution to Exercise B26

First we prove the ‘if’ part. Suppose that (G, \circ) is abelian. We have to show that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G.$$

So let $x, y \in G$. Then

$$\begin{aligned} (x \circ y)^{-1} &= y^{-1} \circ x^{-1} \quad (\text{by Proposition B14}) \\ &= x^{-1} \circ y^{-1} \quad (\text{since } (G, \circ) \text{ is abelian}). \end{aligned}$$

This proves the required statement.

Now we prove the ‘only if’ part. Suppose that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G.$$

We have to show that (G, \circ) is abelian. Let $x, y \in G$. Then

$$\begin{aligned} x \circ y &= ((x \circ y)^{-1})^{-1} \quad (\text{by Proposition B13}) \\ &= (x^{-1} \circ y^{-1})^{-1} \\ &\quad (\text{by the supposition above}) \\ &= (y^{-1})^{-1} \circ (x^{-1})^{-1} \quad (\text{by Proposition B14}) \\ &= y \circ x \quad (\text{by Proposition B13}). \end{aligned}$$

This shows that (G, \circ) is abelian, and completes the required proof.

(There are many different ways to prove the ‘only if’ part here. Here is another way to do it.

Suppose that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G.$$

We have to show that (G, \circ) is abelian. Let $x, y \in G$.

By the supposition above, we have

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1},$$

and by Proposition B14, we have

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

Hence

$$x^{-1} \circ y^{-1} = y^{-1} \circ x^{-1}.$$

Composing both sides on the left and right by x gives

$$x \circ x^{-1} \circ y^{-1} \circ x = x \circ y^{-1} \circ x^{-1} \circ x,$$

that is, by axiom G4,

$$e \circ y^{-1} \circ x = x \circ y^{-1} \circ e,$$

which gives, by axiom G3,

$$y^{-1} \circ x = x \circ y^{-1}.$$

Now composing both sides on the left and right by y gives

$$y \circ y^{-1} \circ x \circ y = y \circ x \circ y^{-1} \circ y,$$

that is, by axiom G4,

$$e \circ x \circ y = y \circ x \circ e,$$

which gives, by axiom G3,

$$x \circ y = y \circ x.$$

Hence (G, \circ) is abelian.)

Solution to Exercise B27

(a) The second row and the second column repeat the borders of the table, so the identity is E .

(b) The first row and the first column repeat the borders of the table, so the identity is D .

(c) The third row and the third column repeat the borders of the table, so the identity is w .

Solution to Exercise B28

Let g be any group element; we will consider the column corresponding to g . Let h also be any group element; we will show that h occurs exactly once in this column.

This is equivalent to proving that there is *exactly one* element of the group, x say, such that

$$x \circ g = h,$$

as illustrated below.

	\cdots	g	\cdots
\vdots		\vdots	
x	\cdots	h	\cdots
\vdots		\vdots	

To show that there is *at least* one such element x , let $x = h \circ g^{-1}$. Then

$$\begin{aligned} x \circ g &= h \circ g^{-1} \circ g \\ &= h \circ e \\ &= h, \end{aligned}$$

so $x = h \circ g^{-1}$ has the property $x \circ g = h$, as claimed.

To show that $x = h \circ g^{-1}$ is the *only* element x of the group such that $x \circ g = h$, suppose that x and y are group elements such that

$$x \circ g = h \quad \text{and} \quad y \circ g = h.$$

Then

$$x \circ g = y \circ g,$$

so, by the Right Cancellation Law,

$$x = y.$$

So there is indeed exactly one element x of the group such that $x \circ g = h$, namely $x = h \circ g^{-1}$.

In other words, in the column labelled g , the element h appears exactly once; it appears in the row labelled by the element $h \circ g^{-1}$.

Solution to Exercise B29

(a) The element e does not appear symmetrically with respect to the main diagonal, so the Cayley table is not a group table.

Alternatively, the elements a , b and c do not have inverses. For example, from the row labelled a we see that the only possible candidate for a^{-1} is c , since $a \circ c = e$; but from the row labelled c we see that $c \circ a = d \neq e$, so a has no inverse.

(b) The element d occurs twice in the row labelled b (and also twice in the column labelled b), so the Cayley table is not a group table.

Solution to Exercise B30

(a) The group table is symmetric with respect to the main diagonal, so this group is abelian.

The table of inverses is as follows.

Element	e	a	b	c	d	f	g	h
Inverse	e	a	b	c	d	f	g	h

(b) The group is non-abelian; for example, $a \circ d = f$, but $d \circ a = h$.

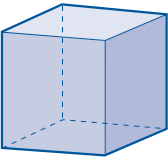
The table of inverses is as follows.

Element	e	a	b	c	d	f	g	h
Inverse	e	c	b	a	g	h	d	f

Solution to Exercise B31

In each case, we use Strategy B1.

Cube

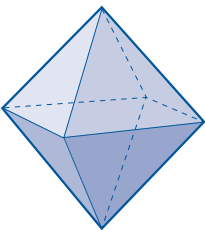


The cube has six faces.

Each face of the cube is a square, and so has eight symmetries (since the order of $S(\square)$ is 8).

It follows from the strategy that the number of symmetries of the cube is $6 \times 8 = 48$.

Octahedron

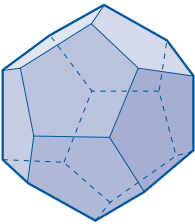


The octahedron has eight faces.

Each face of the octahedron is an equilateral triangle, and so has six symmetries (since the order of $S(\triangle)$ is 6).

It follows from the strategy that the number of symmetries of the octahedron is $8 \times 6 = 48$.

Dodecahedron

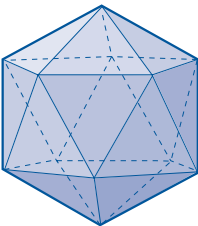


The dodecahedron has 12 faces.

Each face of the dodecahedron is a regular pentagon, and so has 10 symmetries (since the order of $S(\pentagon)$, the symmetry group of the regular pentagon, is 10).

It follows from the strategy that the number of symmetries of the dodecahedron is $12 \times 10 = 120$.

Icosahedron



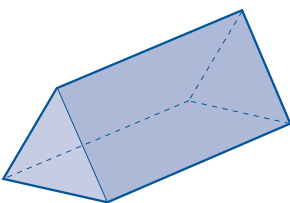
The icosahedron has 20 faces.

Each face of the icosahedron is an equilateral triangle, and so has six symmetries.

It follows from the strategy that the number of symmetries of the icosahedron is $20 \times 6 = 120$.

Solution to Exercise B32

We use Strategy B2.



The triangular prism has two (congruent) equilateral triangle faces and three (congruent) rectangular faces, so there are two ways of applying the strategy.

Consider the equilateral triangle faces.

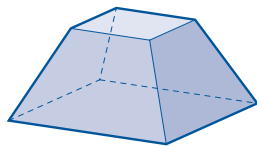
1. The prism has two equilateral triangle faces.
2. Each of the six symmetries of a face of this type gives a symmetry of the whole prism.
3. Hence the number of symmetries of the triangular prism is $2 \times 6 = 12$.

Alternatively, consider the rectangular faces.

1. The prism has three rectangular faces.
2. Each of the four symmetries of a face of this type gives a symmetry of the whole prism.
3. Hence the number of symmetries of the triangular prism is $3 \times 4 = 12$.

Solution to Exercise B33

We can use Strategy B2.



Consider one of the square faces, say the larger one.

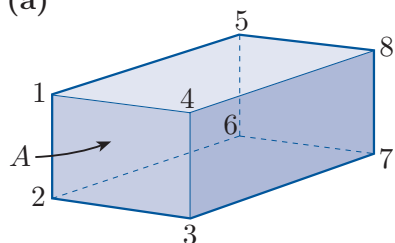
1. The solid has one face of this type.
2. Each of the eight symmetries of this face gives a symmetry of the whole solid.
3. Hence the number of symmetries of the solid is $1 \times 8 = 8$.

Alternatively, consider the trapezium faces.

1. The solid has four trapezium faces.
2. Each trapezium face has two symmetries (the identity and a reflection). Each of these two symmetries gives a symmetry of the whole solid.
3. Hence the number of symmetries of the solid is $4 \times 2 = 8$.

Solution to Exercise B34

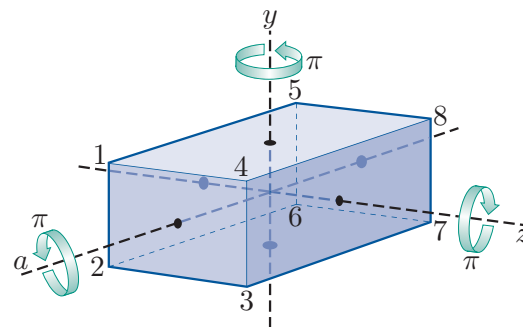
(a)



We use Strategy B2 to count the number of symmetries of the cuboid. The cuboid has six faces – three pairs of opposite faces. Opposite faces are congruent rectangles, and adjacent faces are not congruent. We choose one pair of opposite faces.

1. The cuboid has two faces of the type denoted by A in the diagram above.
2. Each of these faces is a rectangle, and so has four symmetries. Each of these symmetries gives a symmetry of the whole cuboid.
3. Hence the number of symmetries of the cuboid is $2 \times 4 = 8$.

(b) The cuboid has indirect symmetries, so it has four direct symmetries and four indirect symmetries. We first find the direct symmetries. The non-trivial direct symmetries are the rotations a , y and z through π about the axes shown below.



The two-line symbols for the direct symmetries are

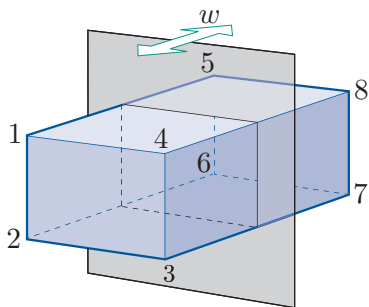
$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix},$$

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \end{pmatrix},$$

$$y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

We can obtain the four indirect symmetries by composing each of these direct symmetries with the reflectional symmetry w in the vertical plane shown below.



This symmetry is

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix},$$

so the four indirect symmetries are

$$w = e \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix},$$

$$x = a \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \end{pmatrix},$$

$$r = y \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{pmatrix},$$

$$s = z \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}.$$

(Three of these four indirect symmetries, namely w , r and s , are reflections in a plane parallel to a pair of opposite faces. Although the other indirect symmetry, x , interchanges pairs of points, it is not a reflection in a plane. It is the composite of a rotational symmetry and a reflection in a plane.)

Unit B2

Subgroups and isomorphisms

Introduction

In Unit B1 *Symmetry and groups* you met the idea of a group and studied a few basic properties of groups. In this unit you will be introduced to many of the fundamental ideas of group theory.

First you will meet the idea of a *subgroup* of a group. This is a group whose elements form a subset of the set of elements of another group, and whose binary operation is the same as for the other group. You will go on to look at what happens when a group element is repeatedly composed with itself, and see how this leads to a way of finding some of the subgroups of a group. You will also explore some properties of *cyclic groups*, which are groups in which every element can be obtained by repeatedly composing one particular element with itself. Finally, you will look at the idea that two groups may differ in their elements and binary operations, but have exactly the same underlying structure, so that, in an abstract sense, they are ‘the same group’.

All the ideas covered in this unit help us gain insight into the structures of groups, enabling us to see and analyse some of the fundamental similarities and differences between various groups.

1 Subgroups

In this section you will see that groups can contain other groups.

1.1 What is a subgroup?

To illustrate the idea of a subgroup, let us consider the symmetry group of the equilateral triangle, $(S(\triangle), \circ)$, which you met in Unit B1. Recall that $S(\triangle) = \{e, a, b, r, s, t\}$, where the letters stand for the symmetries illustrated in Figure 1, and that \circ represents function composition. The group table for $(S(\triangle), \circ)$ is as follows.

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

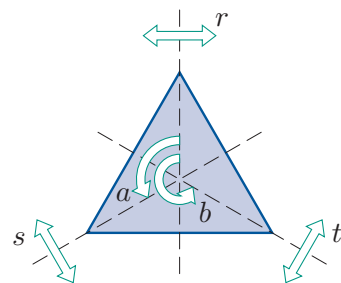


Figure 1 $S(\triangle)$

Now consider the set $\{e, a, b\}$ of *direct* symmetries of the equilateral triangle. We can obtain a Cayley table for this set under function composition by deleting the rows and columns labelled by the indirect symmetries in the group table of $(S(\triangle), \circ)$, as shown below.

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$(S(\triangle), \circ)$

\longrightarrow

\circ	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$(\{e, a, b\}, \circ)$

Let us check whether $(\{e, a, b\}, \circ)$ is a group. Here is a reminder of the group axioms.

Definition

Let G be a set and let \circ be a binary operation defined on G . Then (G, \circ) is a **group** if the following four axioms hold.

G1 Closure For all g, h in G ,

$$g \circ h \in G.$$

G2 Associativity For all g, h, k in G ,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

G3 Identity There is an element e in G such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for \circ on G .)

G4 Inverses For each element g in G , there is an element h in G such that

$$g \circ h = e = h \circ g.$$

(The element h is an **inverse element** of g with respect to \circ .)

We now check these axioms for $(\{e, a, b\}, \circ)$.

G1 Closure The only elements in the body of the Cayley table for $(\{e, a, b\}, \circ)$ are e, a and b , so $\{e, a, b\}$ is closed under function composition; that is, axiom G1 holds.

G2 Associativity We know that function composition is an associative binary operation, so axiom G2 holds.

G3 Identity The row and column labelled e in the Cayley table for $(\{e, a, b\}, \circ)$ repeat the table borders, so e is an identity element for $(\{e, a, b\}, \circ)$; that is, axiom G3 holds.

G4 Inverses We can see from the Cayley table for $(\{e, a, b\}, \circ)$ that each element of $\{e, a, b\}$ has an inverse element in $\{e, a, b\}$ (e is self-inverse and a and b are inverses of each other), so axiom G4 holds.

So all four group axioms hold, and hence $(\{e, a, b\}, \circ)$ is a group.

Since $\{e, a, b\}$ is a subset of $S(\triangle) = \{e, a, b, r, s, t\}$, and both these sets are groups under the same binary operation (namely function composition), we say that $(\{e, a, b\}, \circ)$ is a *subgroup* of $(S(\triangle), \circ)$. In general, we have the following definition.

Definition

A **subgroup** of a group (G, \circ) is a group (H, \circ) , where H is a subset of G .

Notice that it is part of the definition of a subgroup that the subgroup has the *same* binary operation as the original group.

Now consider the subset $\{e, b\}$ of $S(\triangle)$. We can obtain a Cayley table for $(\{e, b\}, \circ)$ in the same way as we did for $(\{e, a, b\}, \circ)$. That is, we start with the group table of $(S(\triangle), \circ)$, and delete the rows and columns labelled by the elements of $S(\triangle)$ that are not elements of $\{e, b\}$, as follows.

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$(S(\triangle), \circ)$

\longrightarrow

\circ	e	b
e	e	b
b	b	a

$(\{e, b\}, \circ)$

The Cayley table for $(\{e, b\}, \circ)$ contains the element a , which is not in the set $\{e, b\}$. So $\{e, b\}$ is not closed under function composition; that is, axiom G1 fails. Thus $(\{e, b\}, \circ)$ is *not* a subgroup of $(S(\triangle), \circ)$.

Exercise B35

For each of the following, construct a Cayley table by deleting rows and columns of the group table for $(S(\triangle), \circ)$, and determine whether the given set and binary operation form a subgroup of $(S(\triangle), \circ)$.

- (a) $(\{e, s\}, \circ)$ (b) $(\{e, b, r\}, \circ)$

Among the groups you met in Unit B1, some are subgroups of others. For example,

$(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$,

since $\mathbb{R} \subseteq \mathbb{C}$ and the binary operations of $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are the same. Similarly,

$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$, and

(\mathbb{Q}^*, \times) is a subgroup of (\mathbb{R}^*, \times) .

In contrast,

(\mathbb{R}^*, \times) is *not* a subgroup of $(\mathbb{R}, +)$.

This is because, although \mathbb{R}^* is a subset of \mathbb{R} , the binary operations of the two groups are different.

In fact, every group (G, \circ) with more than one element has at least two subgroups: the group (G, \circ) itself, and the group $(\{e\}, \circ)$, known as the **trivial subgroup**, whose only element is the identity element. Some particular examples of the trivial subgroup of a group include:

the trivial subgroup $(\{e\}, \circ)$ of the group $(S(\triangle), \circ)$,

the trivial subgroup $(\{0\}, +)$ of the group $(\mathbb{Z}, +)$,

the trivial subgroup $(\{1\}, \times)$ of the group (\mathbb{R}^*, \times) .

A subgroup of a group (G, \circ) other than the whole group (G, \circ) is called a **proper subgroup**.

A subgroup (H, \circ) of an abelian group (G, \circ) is always abelian, because if $x \circ y = y \circ x$ for all elements x and y of G , then it must also be true that $x \circ y = y \circ x$ for all elements x and y of the subset H of G .

However, a non-abelian group can have an abelian subgroup. This is illustrated by the example at the start of this subsection: $(S(\triangle), \circ)$ is non-abelian but its subgroup $(\{e, a, b\}, \circ)$ is abelian, as you can see by looking at their group tables. (Recall that a finite group is abelian if and only if its group table is symmetric with respect to the main diagonal.)

Some texts use the notation $H \leq G$ to assert that H is a subgroup of G and the notation $H < G$ to assert that H is a proper subgroup of G , but we will not use these notations in M208.

Identities and inverses in subgroups

We now need to deal with two rather subtle issues that arise from the definition of a subgroup.

Consider a group (G, \circ) , with identity element e , and suppose that (H, \circ) is a subgroup of (G, \circ) . Might the identity element of (H, \circ) be an element other than e ? In fact, this is *not* possible, as stated and proved below. The identity element of (H, \circ) must be the same element as the identity element of (G, \circ) .

A similar issue arises with inverses of group elements. Again, consider a group (G, \circ) and a subgroup (H, \circ) . Might there be an element h of H whose inverse in (H, \circ) is a different element from its inverse in (G, \circ) ? Again, this is *not* possible, as stated and proved below.

Theorem B23

Let (G, \circ) be a group with a subgroup (H, \circ) .

- (a) The identity element of (H, \circ) is the same as the identity element of (G, \circ) .
- (b) For each element h of H , the inverse of h in (H, \circ) is the same as its inverse in (G, \circ) .

Proof

- (a) Let the identity elements of (G, \circ) and (H, \circ) be e and e_H , respectively. Then $e_H \circ e_H = e_H$ (since e_H is the identity element of (H, \circ)), and $e \circ e_H = e_H$ (since e is the identity element of (G, \circ) , and $e_H \in G$). It follows that $e_H \circ e_H = e \circ e_H$, and hence, by the Right Cancellation Law, $e_H = e$.
- (b) Let $h \in H$, and suppose that the inverse of h in H is a and the inverse of h in G is b . We know by part (a) that (G, \circ) and (H, \circ) have the same identity element, e say. Thus $h \circ a = e$ and $h \circ b = e$. It follows that $h \circ a = h \circ b$, and hence, by the Left Cancellation Law, $a = b$. ■

1.2 Checking whether a subset forms a subgroup

At the start of the previous subsection you saw that $(\{e, a, b\}, \circ)$ is a subgroup of $(S(\triangle), \circ)$. This was shown by checking each group axiom for $(\{e, a, b\}, \circ)$.

In fact, it was not necessary to carry out such extensive checks, because some properties hold for $(\{e, a, b\}, \circ)$ simply because they hold for $(S(\triangle), \circ)$. For example, we already know that $x \circ e = x = e \circ x$ for any element x of $S(\triangle)$, so the same must be true for any element x of the subset $\{e, a, b\}$ of $S(\triangle)$. So, to check that e is an identity element for $(\{e, a, b\}, \circ)$, all we really need to check is that e actually belongs to $\{e, a, b\}$. (Which of course it does!)

The next theorem sets out exactly what you need to check to show whether or not a subset of a group forms a subgroup.

Theorem B24 Subgroup test

Let (G, \circ) be a group with identity element e , and let H be a subset of G . Then (H, \circ) is a subgroup of (G, \circ) if and only if the following three properties hold.

SG1 Closure For all x, y in H , the composite $x \circ y$ is in H .

SG2 Identity The identity element e of G is in H .

SG3 Inverses For each x in H , its inverse x^{-1} in G is in H .

We refer to the three properties SG1, SG2 and SG3 listed in the theorem as the three **subgroup properties**. Notice that although these properties have the same names as three of the group axioms, namely *Closure*, *Identity* and *Inverses*, only the closure property involves the same ideas as the corresponding group axiom. The other two properties involve only a check that certain elements (the identity element of G and the inverses of elements of H) *actually belong to* H : they do not involve a check that these elements have the defining properties of an identity element or inverse.

Proof of Theorem B24 First we prove the ‘if’ part. Suppose that the three subgroup properties hold. We need to check that (H, \circ) is a group. To do that, we check that (H, \circ) satisfies the four group axioms.

G1 Closure Property SG1 means the same as axiom G1, so axiom G1 holds.

G2 Associativity Since (G, \circ) is a group, we know that

$$x \circ (y \circ z) = (x \circ y) \circ z$$

for all elements x, y, z in G , so this equation holds for all elements x, y, z in the subset H of G . Thus axiom G2 holds.

G3 Identity We have $e \in H$, since property SG2 holds, and if $x \in H$ then $x \circ e = x = e \circ x$, since $x \in G$ and e is the identity element of (G, \circ) . So e is an identity element for \circ on H . Thus axiom G3 holds.

G4 Inverses Let $x \in H$. Then the inverse x^{-1} of x in G is also in H , since property SG3 holds, and we have $x \circ x^{-1} = e = x^{-1} \circ x$. So x^{-1} is an inverse of x in H . Thus axiom G4 holds.

Hence (H, \circ) satisfies the four group axioms, and so is a group.

Now we prove the ‘only if’ part. Suppose that (H, \circ) is a subgroup of (G, \circ) . We have to show that properties SG1, SG2 and SG3 hold. Since (H, \circ) is a group, the set H is closed under \circ , so property SG1 holds. Also, by Theorem B23, H contains the identity element e of G and the inverse of each element of H , so properties SG2 and SG3 hold. ■

Theorem B24 tells us that if (G, \circ) is a group and H is a subset of G , then to check that (H, \circ) is a subgroup of (G, \circ) we need only check that the three subgroup properties hold, rather than having to check the full group axioms. It also tells us that to show that (H, \circ) is *not* a subgroup of (G, \circ) , we just need to show that *any one* of the three subgroup properties fails. (To do this, we give a counter-example, not a general argument.)

Remember that before you apply Theorem B24 you need to be sure that H is a subset of G , and that the binary operations on the two sets are the same. If these conditions do not hold, then (H, \circ) is certainly not a subgroup of (G, \circ) .

The worked example below demonstrates how to use the three subgroup properties to determine whether or not (H, \circ) is a subgroup of a group (G, \circ) , in cases where H is a small finite set. In this situation, particularly if you suspect that (H, \circ) is a subgroup of (G, \circ) , it is often useful to start by constructing a Cayley table for (H, \circ) . You can then use the table to help you check the three subgroup properties. (In the worked example the group (G, \circ) is finite, but the same approach can be used if (G, \circ) is an infinite group.)

Worked Exercise B15

- (a) Show that $(\{e, a, b, c\}, \circ)$ is a subgroup of $(S(\square), \circ)$.
 (b) Show that $(\{e, r, s, t\}, \circ)$ is not a subgroup of $(S(\square), \circ)$.
 (The non-identity elements of $S(\square)$ are shown in Figure 2.)

Solution

- (a) We have $\{e, a, b, c\} \subseteq S(\square)$, and the binary operation \circ is the same on each set.

💡 Construct a Cayley table for $(\{e, a, b, c\}, \circ)$, by deleting the unwanted rows and columns of the group table of $(S(\square), \circ)$ (which is repeated as Table 1). 💡

The Cayley table for $(\{e, a, b, c\}, \circ)$ is as follows.

\circ	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

We check the three subgroup properties.

💡 Use the Cayley table to check properties SG1 and SG3. To check for inverses, look for occurrences of the identity element in the table. 💡

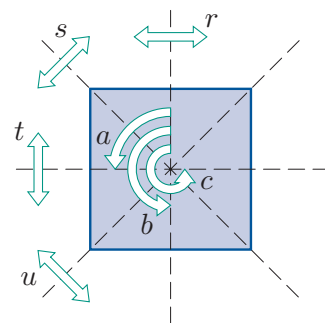


Figure 2 $S(\square)$

Table 1 $S(\square)$

\circ	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

SG1 Closure Every element in the body of the table is in $\{e, a, b, c\}$, so $\{e, a, b, c\}$ is closed under function composition.

SG2 Identity The identity element in $S(\square)$ is e , and $e \in \{e, a, b, c\}$.

SG3 Inverses The elements e and b are self-inverse, and a and c are inverses of each other, so $\{e, a, b, c\}$ contains the inverse of each of its elements.

Hence $(\{e, a, b, c\}, \circ)$ satisfies the three subgroup properties, and so is a subgroup of $(S(\square), \circ)$.

- (b) We have $\{e, r, s, t\} \subseteq S(\square)$, and the binary operation \circ is the same on each set.

However, $r, t \in \{e, r, s, t\}$ but $r \circ t = b \notin \{e, r, s, t\}$, so property SG1 fails.

Hence $(\{e, r, s, t\}, \circ)$ is not a subgroup of $(S(\square), \circ)$.

Exercise B36

Show that $(\{e, b, s, u\}, \circ)$ is a subgroup of $(S(\square), \circ)$.

Many of the exercises and worked exercises in the rest of this subsection involve subsets of the standard groups of numbers that you met in Unit B1. Here is a reminder of these groups.

Standard groups of numbers

Infinite groups

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +), \\ (\mathbb{Q}^*, \times), \quad (\mathbb{R}^*, \times), \quad (\mathbb{C}^*, \times).$$

Finite groups, for any integer $n \geq 2$:

$$(\mathbb{Z}_n, +_n), \\ (U_n, \times_n), \text{ and in particular } (\mathbb{Z}_p^*, \times_p), \text{ where } p \text{ is prime.}$$

Here \mathbb{Q}^* , \mathbb{R}^* , \mathbb{C}^* and \mathbb{Z}_n^* mean \mathbb{Q} , \mathbb{R} , \mathbb{C} and \mathbb{Z}_n with the element 0 removed, and U_n is the set of integers in \mathbb{Z}_n coprime to n .

The next exercise involves a finite subgroup of one of the infinite groups above.

Exercise B37

- (a) Construct a Cayley table for $(\{1, -1, i, -i\}, \times)$ (where $i^2 = -1$).
- (b) Show that $(\{1, -1, i, -i\}, \times)$ is a subgroup of the group (\mathbb{C}^*, \times) .

So far, we have looked at how to check whether (H, \circ) is a subgroup of a group (G, \circ) only in the case where H is finite. If H is an *infinite* set, then we have to check the three subgroup properties by using algebraic arguments rather than a Cayley table. This is demonstrated in the next worked exercise.

Worked Exercise B16

Show that (\mathbb{R}^+, \times) is a subgroup of the group (\mathbb{R}^*, \times) , where \mathbb{R}^+ denotes the set of positive real numbers.

Solution

We have $\mathbb{R}^+ \subseteq \mathbb{R}^*$, and the binary operation \times is the same on each set.

We check the three subgroup properties.

SG1 Closure Let $x, y \in \mathbb{R}^+$; then $x, y \in \mathbb{R}$, $x > 0$ and $y > 0$. It follows that $x \times y \in \mathbb{R}$ and $x \times y > 0$, so $x \times y \in \mathbb{R}^+$. Thus \mathbb{R}^+ is closed under \times .

SG2 Identity The identity element in (\mathbb{R}^*, \times) is 1. Since $1 > 0$, we have $1 \in \mathbb{R}^+$.

SG3 Inverses Let $x \in \mathbb{R}^+$. The inverse of x in (\mathbb{R}^*, \times) is $1/x$. Since $x \in \mathbb{R}^+$, we have $x \in \mathbb{R}$ and $x > 0$. It follows that $1/x \in \mathbb{R}$ and $1/x > 0$, so $1/x \in \mathbb{R}^+$. Thus \mathbb{R}^+ contains the inverse of each of its elements.

Hence (\mathbb{R}^+, \times) satisfies the three subgroup properties, and so is a subgroup of (\mathbb{R}^*, \times) .

The next exercise involves the set of integer multiples of 3; we denote this set by $3\mathbb{Z}$. That is,

$$3\mathbb{Z} = \{3k : k \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}.$$

In general, for any number x , we denote the set of integer multiples of x by $x\mathbb{Z}$. That is,

$$x\mathbb{Z} = \{xk : k \in \mathbb{Z}\} = \{\dots, -2x, -x, 0, x, 2x, 3x, \dots\}.$$

Exercise B38

Show that $(3\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

The solution to Exercise B38 remains valid if the integer 3 is replaced by any integer n , so we have the following result.

For any integer n , $(n\mathbb{Z}, +)$ is a subgroup of the group $(\mathbb{Z}, +)$.

Exercise B39

- (a) Is $(6\mathbb{Z}, +)$ a subgroup of $(\mathbb{Z}, +)$?
- (b) Is $(6\mathbb{Z}, +)$ a subgroup of $(2\mathbb{Z}, +)$?
- (c) Is $(5\mathbb{Z}, +)$ a subgroup of $(3\mathbb{Z}, +)$?

Justify your answers.

In the next worked exercise, Theorem B24 (Subgroup test) is used to show that a particular infinite subset is *not* a subgroup of a particular infinite group.

Worked Exercise B17

Show that $(\mathbb{Z}^+, +)$ is not a subgroup of the group $(\mathbb{Z}, +)$, where \mathbb{Z}^+ denotes the set of positive integers.

Solution

We have $\mathbb{Z}^+ \subseteq \mathbb{Z}$, and the binary operation $+$ is the same on each set.

However, the identity element in $(\mathbb{Z}, +)$ is 0, but $0 \notin \mathbb{Z}^+$, so property SG2 fails.

Hence $(\mathbb{Z}^+, +)$ is not a subgroup of $(\mathbb{Z}, +)$.

Exercise B40

- (a) Show that (\mathbb{Q}^*, \times) is not a subgroup of the group (\mathbb{R}^+, \times) .
(You saw that (\mathbb{R}^+, \times) is a group in Worked Exercise B16.)
- (b) Show that $(W, +)$ is not a subgroup of the group $(\mathbb{Z}, +)$, where W is the set of non-negative integers.

The following two exercises should familiarise you further with checking the subgroup properties.

Exercise B41

Show that $(H, +_{12})$ is a subgroup of the group $(\mathbb{Z}_{12}, +_{12})$, where $H = \{0, 3, 6, 9\}$.

Hint: In this case, it is easier to construct the Cayley table for $(H, +_{12})$ directly, rather than by deleting rows and columns from the group table for $(\mathbb{Z}_{12}, +_{12})$.

Exercise B42

In each of the following cases, H is a subset of G , but (H, \circ) is not a subgroup of the group (G, \circ) . Explain why not.

- (a) $(G, \circ) = (S(\square), \circ)$ and $(H, \circ) = (\{e, a, c\}, \circ)$.
(The non-identity elements of $S(\square)$ are shown in Figure 3.)
- (b) $(G, \circ) = (\mathbb{Z}_5^*, \times_5)$ and $(H, \circ) = (\{2, 3, 4\}, \times_5)$.
- (c) $(G, \circ) = (\mathbb{R}^*, \times)$ and $(H, \circ) = (\mathbb{Z}^*, \times)$.

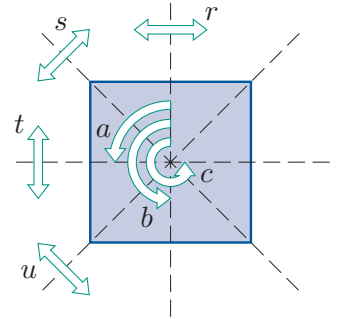


Figure 3 $S(\square)$

An unfamiliar binary operation

The final worked exercise and exercise in this subsection involve subsets of a group with an unfamiliar binary operation. They give you an opportunity to revise checking all the group axioms, as well as to practise checking the three subgroup properties.

Worked Exercise B18

Let X be the subset of \mathbb{R}^2 consisting of all the points not on the y -axis; that is,

$$X = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}.$$

Let $*$ be the binary operation on X defined by

$$(a, b) * (c, d) = (ac, ad + b).$$



For example, $(2, 5) * (4, 3) = (2 \times 4, 2 \times 3 + 5) = (8, 11)$.

- (a) Show that $(X, *)$ is a group.
- (b) Determine whether each of the following subsets of X together with the binary operation $*$ forms a subgroup of $(X, *)$.
 - (i) $A = \{(a, b) \in X : a = 1\}$
 - (ii) $B = \{(a, b) \in X : b = 1\}$

Solution



(a) We check the four group axioms.

G1 Closure

 If we combine two elements of X using $*$, do we get another element of X ? To check this, start with two general elements of X and combine them. 



Let $(a, b), (c, d) \in X$; then $a, b, c, d \in \mathbb{R}$, and $a \neq 0$ and $c \neq 0$. We have

$$(a, b) * (c, d) = (ac, ad + b).$$

 To check that this point is in X , we have to check that it is in \mathbb{R}^2 and its first coordinate is non-zero. 

Now $(ac, ad + b) \in \mathbb{R}^2$ because $a, b, c, d \in \mathbb{R}$, and $ac \neq 0$ because $a \neq 0$ and $c \neq 0$, so $(ac, ad + b) \in X$. Thus X is closed under $*$.

G2 Associativity

 Since $*$ is an unfamiliar binary operation, we must use an algebraic argument to prove associativity. 

Let $(a, b), (c, d), (e, f) \in X$. We have

$$\begin{aligned}(a, b) * ((c, d) * (e, f)) &= (a, b) * (ce, cf + d) \\ &= (ace, acf + ad + b)\end{aligned}$$

and

$$\begin{aligned}((a, b) * (c, d)) * (e, f) &= (ac, ad + b) * (e, f) \\ &= (ace, acf + ad + b).\end{aligned}$$

The two expressions obtained are the same, so $*$ is associative on X .

G3 Identity

 Try to find a likely candidate to be an identity. 

Suppose that (e, f) is an identity in X . Then we must have, for each $(a, b) \in X$,

$$(a, b) * (e, f) = (a, b) = (e, f) * (a, b).$$

The left-hand equation gives

$$(ae, af + b) = (a, b).$$

Comparing coordinates gives

$$ae = a \quad \text{and} \quad af + b = b;$$

that is,

$$ae = a \quad \text{and} \quad af = 0.$$

Since these equations must hold for all non-zero values of a , we must have $e = 1$ and $f = 0$. So the only possibility for an identity is $(1, 0)$.

☁️ Now check to see whether this point actually is an identity. ☁️

Now $(1, 0) \in X$, since it is in \mathbb{R}^2 and its first coordinate is non-zero, and for all $(a, b) \in X$, we have

$$(a, b) * (1, 0) = (a \times 1, a \times 0 + b) = (a, b)$$

and

$$(1, 0) * (a, b) = (1 \times a, 1 \times b + 0) = (a, b).$$

So $(1, 0)$ is an identity for $*$ on X .

G4 Inverses

☁️ Try to find a likely candidate to be an inverse of a general element $(a, b) \in X$. ☁️

Let $(a, b) \in X$; then $a \neq 0$. Suppose that (c, d) is an inverse of (a, b) . Then we must have

$$(a, b) * (c, d) = (1, 0) = (c, d) * (a, b).$$

The left-hand equation gives

$$(ac, ad + b) = (1, 0).$$

Comparing coordinates gives

$$ac = 1 \quad \text{and} \quad ad + b = 0.$$

☁️ Try to find c and d in terms of a and b . ☁️

Since $a \neq 0$, these equations give

$$c = \frac{1}{a} \quad \text{and} \quad d = -\frac{b}{a}.$$

So the only possibility for an inverse of (a, b) is $(1/a, -b/a)$.

☁️ Now check to see whether this point actually is an inverse of (a, b) . ☁️

Now $(1/a, -b/a) \in X$, since it is in \mathbb{R}^2 (because a and b are in \mathbb{R} and a is non-zero) and its first coordinate is non-zero, and we have

$$(a, b) * \left(\frac{1}{a}, -\frac{b}{a}\right) = \left(a \times \frac{1}{a}, a \times \left(-\frac{b}{a}\right) + b\right) = (1, 0)$$

and

$$\left(\frac{1}{a}, -\frac{b}{a}\right) * (a, b) = \left(\frac{1}{a} \times a, \frac{1}{a} \times b - \frac{b}{a}\right) = (1, 0).$$

So $(1/a, -b/a)$ is an inverse of (a, b) . Thus every element of X has an inverse in X .

Hence $(X, *)$ satisfies the four group axioms, and so is a group.



- (b) (i)  Simplify the description of A , if possible, to make it easier to work with. 

We have

$$A = \{(a, b) \in X : a = 1\} = \{(1, b) : b \in \mathbb{R}\}.$$

We check the three subgroup properties for A .

SG1 Closure

 Start with two general elements of A , combine them using $*$, and check that the result is in A . 

Let $(1, b), (1, d) \in A$. We have

$$(1, b) * (1, d) = (1 \times 1, 1 \times d + b) = (1, d + b).$$

This point is in A because its first coordinate is 1. Thus A is closed under $*$.

SG2 Identity

The identity element in $(X, *)$ is $(1, 0)$. This point has first coordinate 1, so it is in A .

SG3 Inverses

Let $(1, b) \in A$. By the solution to part (a), the inverse of $(1, b)$ in $(X, *)$ is

$$\left(\frac{1}{1}, -\frac{b}{1}\right) = (1, -b).$$



This point has first coordinate 1, so it is in A . Thus A contains the inverse of each of its elements.

Hence $(A, *)$ satisfies the three subgroup properties, and so is a subgroup of $(X, *)$.

- (ii)  Simplify the description of B , if possible, to make it easier to work with. 

We have

$$B = \{(a, b) \in X : b = 1\} = \{(a, 1) : a \in \mathbb{R}, a \neq 0\}.$$

 We can see immediately that the identity $(1, 0)$ of $(X, *)$ is not in B , so there is no need to check the other subgroup properties. 

The identity in $(X, *)$ is $(1, 0)$, but this point is not in B , so property SG2 fails.

Hence $(B, *)$ is not a subgroup of $(X, *)$.

The group $(X, *)$ defined in Worked Exercise B18 is non-abelian, as you can check by working out $(1, 1) * (2, 2)$ and $(2, 2) * (1, 1)$ for example. In contrast, the different group $(X, *)$ defined in the next exercise is abelian, because for this group $(a, b) * (c, d) = (c, d) * (a, b)$ for all $(a, b), (c, d) \in X$.

Exercise B43

Let X be the set

$$X = \{(a, b) \in \mathbb{R}^2 : a, b \neq 0\}$$

and let $*$ be the binary operation on X defined by

$$(a, b) * (c, d) = (ac, bd).$$

- (a) Show that $(X, *)$ is a group.
- (b) Determine whether each of the following subsets of X together with the binary operation $*$ forms a subgroup of $(X, *)$.
 - (i) $A = \{(a, b) \in X : a = 1\}$
 - (ii) $B = \{(a, b) \in X : a + b = 2\}$

When we are discussing groups, and subgroups of groups, it can be cumbersome to keep using notation of the form (G, \circ) , in which both the set of the group and the binary operation are included. For this reason, from now on we will often use the following convention.

Convention

We can refer to a group (G, \circ) simply as G , as long as the binary operation is clear from the context.

So we might say, for example:

- ‘the subgroup H of the group G ’
- ‘the symmetry group $S(F)$ of the figure F ’
- ‘the set H is a subgroup of the group G ’
- ‘the set $\{e, a, b, c\}$ is a subgroup of the group G ’.

When you see phrases like these, or when you use them yourself, you should keep in mind that a group is definitely *not just a set*, but consists of both a set and a binary operation. When you are reading about a group or working with a group it is important that you know what the binary operation is.

Because of the convention above, if (G, \circ) is a group then an instance of the notation G could mean either the group (G, \circ) or simply the set G . Often it does not matter which meaning applies; for example, this is the case for the statement ‘Let g be an element of G .’ If it does matter, then the meaning should be clear from the context.

1.3 Subgroups of symmetry groups

In Unit B1 you saw that the symmetries of any figure F in \mathbb{R}^2 or \mathbb{R}^3 form a group under function composition called the **symmetry group** of F and denoted by $S(F)$. In this subsection we will look at some ways in which we can find subgroups of the symmetry group of a figure.

The subgroup of direct symmetries of a figure

First, as stated in the theorem below, the set $S^+(F)$ of *direct* symmetries of a figure F always forms a subgroup of its symmetry group $S(F)$. Of course, if the figure F has no indirect symmetries, then $S^+(F)$ and $S(F)$ are the same set.

Theorem B25

Let F be a figure in \mathbb{R}^2 or \mathbb{R}^3 . Then the set $S^+(F)$ of direct symmetries of F is a subgroup of the symmetry group $S(F)$ of F .

Proof We have $S^+(F) \subseteq S(F)$, and the binary operation \circ is the same on each set. We check the three subgroup properties, using the properties of direct and indirect symmetries given in Subsection 1.4 of Unit B1.

SG1 Closure Composing any two direct symmetries gives a direct symmetry, so $S^+(F)$ is closed under \circ .

SG2 Identity The identity element e of $S(F)$ is a direct symmetry, so it is in $S^+(F)$.

SG3 Inverses If f is a direct symmetry, then f^{-1} is also a direct symmetry. So $S^+(F)$ contains the inverse of each of its elements.

Hence $S^+(F)$ satisfies the three subgroup properties, and so is a subgroup of $S(F)$. ■

For example, the set $S^+ = \{e, a, b\}$ of direct symmetries of the equilateral triangle is a subgroup of the symmetry group $S(\triangle)$ of the equilateral triangle, as you saw at the start of this unit.

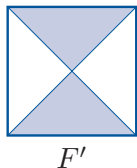
Modifying a figure

Another way in which we can sometimes find subgroups of a symmetry group $S(F)$ is to modify the figure F to restrict its symmetry. We could, for example, modify a square F by introducing a pattern of shapes, as illustrated in Worked Exercise B19 below. The modified square F' is still a plane figure (a subset of \mathbb{R}^2): it consists of all the points that lie on the lines or in the shaded areas. The symmetry group $S(F')$ of the modified square consists of those symmetries of the square that leave the pattern of shapes unchanged.

Worked Exercise B19

Let F' be the modified square shown below. Write down a subgroup of $S(\square)$ by listing the symmetries of the figure F' .

(For convenience, Figure 4 shows the non-identity elements of $S(\square)$.)



Solution

The effect of the modification is that the rotations a and c and the reflections s and u , which are symmetries of the unmodified square, are no longer symmetries of the figure.

A subgroup of $S(\square)$ is

$$S(F') = \{e, b, r, t\}.$$

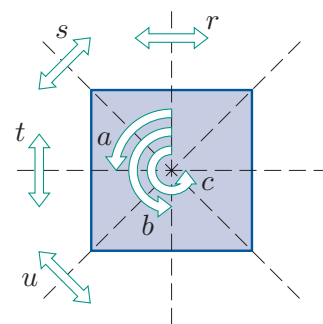
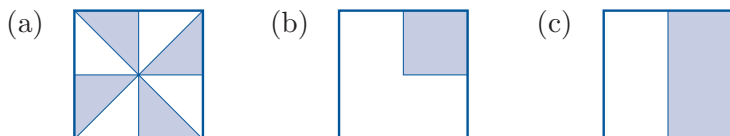


Figure 4 $S(\square)$

Exercise B44

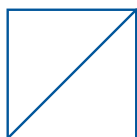
Write down three subgroups of $S(\square)$ by listing the elements of the symmetry groups of each of the following modified squares.



We often use a simple pattern of line segments to restrict the symmetries of a figure. In the following worked exercise, a single diagonal line is used to restrict the symmetries of a square. Again, the modified square F' is still a plane figure: in this case it consists of all the points that lie on the lines.

Worked Exercise B20

Write down a subgroup of $S(\square)$ by listing the symmetries of the following modified square F' .



Solution

The effect of adding the diagonal line is that the rotations a and c and the reflections r and t , which are symmetries of the unmodified square, are no longer symmetries of the figure.

A subgroup of $S(\square)$ is

$$S(F') = \{e, b, s, u\}.$$

Exercise B45

Let F be a regular hexagon. Describe geometrically the elements of the subgroup $S(F')$ of $S(F)$, where F' is the figure obtained by inscribing an equilateral triangle inside F as shown.

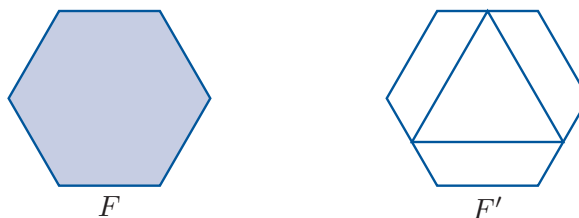


Figure 5 The square with its usual location labels

Fixing a feature of a figure

A third possible way to find a subgroup of a symmetry group $S(F)$ is to fix some feature of the figure, such as a vertex or an edge. That is, we consider only the elements of $S(F)$ that map that feature to itself. For example, consider the square with its usual vertex location labels, as shown in Figure 5. If we fix the vertex at location 1, that is, if we consider only the symmetries that map this vertex to itself, then we obtain the subset $\{e, s\}$ of $S(\square)$. Fixing a subset of a figure always yields a subgroup of the symmetry group of the figure, as stated in the theorem below.

The feature of a figure that we fix can consist of any subset of the points that make up the figure. If the subset consists of more than one point, then the subset can be fixed without every individual point in the subset being fixed. For example, for the square in Figure 5, if we fix the edge that joins the vertices at locations 1 and 4, then we obtain the subset $\{e, r\}$ of $S(\square)$. The symmetry r fixes the edge described, even though it does not fix each point on this edge.

Theorem B26

Let F be a figure in \mathbb{R}^2 or \mathbb{R}^3 and let A be a subset of F . Then the subset of $S(F)$ whose elements are all the symmetries of F that fix A is a subgroup of $S(F)$.

Proof Let H be the subset of $S(F)$ described. We show that the three subgroup properties hold for H .

SG1 Closure Let f and g be symmetries of F that fix A . Then $g \circ f$ also fixes A . Hence H is closed under function composition.

SG2 Identity The identity symmetry fixes A , so H contains the identity element of $S(F)$.

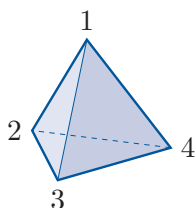
SG3 Inverses Let f be a symmetry of F that fixes A . Then f^{-1} also fixes A . Thus H contains the inverse of each of its elements.

Hence H satisfies the three subgroup properties, and so is a subgroup of $S(F)$. ■

We now use the method of fixing vertices to find some subgroups of the symmetry group of a regular tetrahedron, which we will denote by $S(\text{tet})$. You met the symmetries of the regular tetrahedron in Subsection 5.3 of Unit B1, and you may find it helpful to refresh your memory of these before continuing. As in Unit B1, we specify a symmetry in $S(\text{tet})$ by using a two-line symbol that indicates how the vertex at each location is affected by the symmetry.

Worked Exercise B21

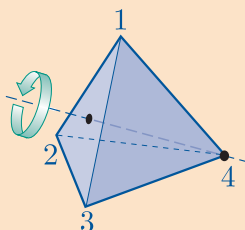
Consider the labelled regular tetrahedron shown below.



Write down, as two-line symbols, the elements of the subgroup of $S(\text{tet})$ that consists of the symmetries of the tetrahedron that fix the vertex at location 4.

Solution

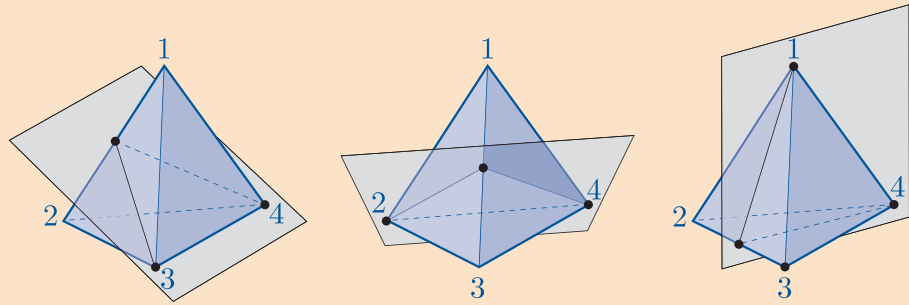
☁ The direct symmetries of the tetrahedron that fix the vertex at location 4 are the three rotations through 0 , $2\pi/3$ and $4\pi/3$ radians about the line through this vertex and the centre of the opposite face.



These are the symmetries

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

The indirect symmetries that fix the vertex at location 4 are reflections in three planes. Each such plane contains one of the three edges that meet at the vertex at location 4, and passes through the midpoint of the opposite edge.



These are the symmetries

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

The required subgroup is

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \right\}.$$

Notice that the elements of the subgroup in Worked Exercise B21 look exactly like the elements of $S(\triangle)$, the symmetry group of an equilateral triangle, written as two-line symbols, but with an extra column, mapping 4 to 4, at the end. This is because each symmetry of the tetrahedron that fixes the vertex at location 4 gives a symmetry of the face with vertices at locations 1, 2 and 3.

In a similar way, we can find subgroups of $S(\text{tet})$ that fix the vertices at locations 1, 2 and 3, respectively. The elements of the subgroup that fixes the vertex at location 1 look like the elements of $S(\triangle)$ written as two-line symbols, but with the vertices of the triangle labelled 2, 3 and 4, and with an extra column mapping 1 to 1. Similar descriptions apply to the other two subgroups.

Exercise B46

Write down, as two-line symbols, the elements of the subgroup of $S(\text{tet})$ that consists of the symmetries of the tetrahedron shown in Worked Exercise B21 that fix the vertex at location 3.

Exercise B47

Write down, as two-line symbols, the elements of the subgroup of $S(\text{tet})$ that consists of the symmetries of the tetrahedron shown in Worked Exercise B21 that fix the edge joining the vertices at locations 1 and 2.

The strategy below summarises the methods that you have seen for finding subgroups of the symmetry group of a figure.

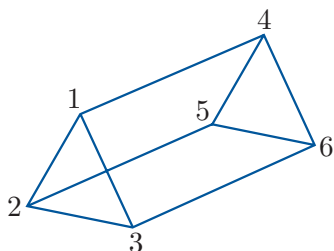
Strategy B3

To find a subgroup of the symmetry group of a figure in \mathbb{R}^2 or \mathbb{R}^3 , do *one* of the following.

- Find the direct symmetries of the figure.
- Modify the figure to restrict its symmetry; for example, introduce a pattern of lines or shapes. Then determine which of the symmetries of the original figure are symmetries of the new figure.
- Find the symmetries of the figure that fix a particular vertex (or any other particular subset of the figure).

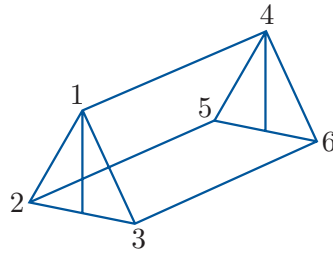
Exercise B48

Let F be the wire framework of a triangular prism, labelled as shown below. The triangles at its ends are equilateral, and its other faces are rectangles.

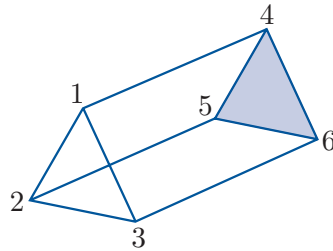


Find three subgroups of $S(F)$ by considering the following ways of restricting the symmetry. Give each symmetry as a two-line symbol.

- (a) Add a vertical wire to each of the triangular ends of the framework prism, as shown below.



- (b) Fill in a triangular face at one end of the framework prism, as shown below.



- (c) Fix the vertices at locations 1 and 4.

2 Order of a group element

In this section we will explore what happens when we take an element of a group and repeatedly combine it with itself.

2.1 Powers of a group element

Before we can proceed, we need a notation for writing down repeated combinations of an element. We normally use index notation. If (G, \circ) is a group, and x is an element of G , then we write

x^2 to represent $x \circ x$,

x^3 to represent $x \circ x \circ x$,

x^4 to represent $x \circ x \circ x \circ x$,

and so on. We interpret x^1 to mean just x itself, and x^0 to mean e , the identity element of G .

We also attach a meaning to negative powers of a group element. You have seen that x^{-1} represents the inverse of x . We also write

x^{-2} to represent $x^{-1} \circ x^{-1}$,

x^{-3} to represent $x^{-1} \circ x^{-1} \circ x^{-1}$,

x^{-4} to represent $x^{-1} \circ x^{-1} \circ x^{-1} \circ x^{-1}$,

and so on.

Here is a summary of this notation.

Powers of a group element

Powers of an element x of a group (G, \circ) are defined as follows.

Let n be a positive integer. Then

$$x^0 = e, \quad \text{the identity element}$$

$$x^n = \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ copies of } x}$$

$$x^{-n} = \underbrace{x^{-1} \circ x^{-1} \circ \cdots \circ x^{-1}}_{n \text{ copies of } x^{-1}}.$$

Each power of x is an element of G , since G is closed under \circ .

Worked Exercise B22

Find the following powers in the group $S(\square)$:

$$c^0, c^1, c^2, c^3, c^4, c^5.$$

(The non-identity elements of $S(\square)$ are shown in Figure 6.)

Solution

$$\begin{aligned} c^0 &= e, & c^4 &= c \circ c \circ c \circ c \\ c^1 &= c, & &= c^3 \circ c \\ & & &= a \circ c \\ c^2 &= c \circ c & &= e, \\ &= b, & c^5 &= c \circ c \circ c \circ c \circ c \\ c^3 &= c \circ c \circ c & &= c^4 \circ c \\ &= c^2 \circ c & &= e \circ c \\ &= b \circ c & &= c. \\ &= a, \end{aligned}$$

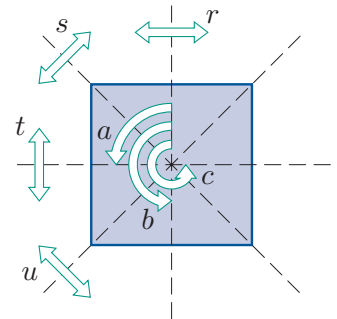


Figure 6 $S(\square)$

Exercise B49

Find the following powers in the group $S(\square)$.

- (a) $a^0, a^1, a^2, a^3, a^4, a^5$
- (b) $a^{-1}, a^{-2}, a^{-3}, a^{-4}, a^{-5}$
- (c) b^0, b^1, b^2, b^3, b^4
- (d) b^{-1}, b^{-2}, b^{-3}
- (e) r^0, r^1, r^2, r^3, r^4

The following familiar index laws hold for the powers of a group element.

Theorem B27 Index laws

Let x be an element of a group (G, \circ) , and let m and n be integers. The following index laws hold.

- (a) $x^m \circ x^n = x^{m+n}$
- (b) $(x^m)^n = x^{mn}$
- (c) $(x^n)^{-1} = x^{-n} = (x^{-1})^n$

Proof Proofs of the laws in the case where m and n are positive integers are given or commented on below. The other cases, where m and n might be zero or negative, can be proved in similar ways, using the definitions of x^0 and negative powers of x . The details are omitted here.

Let x be an element of a group (G, \circ) , and let m and n be positive integers.

(a) We have

$$\begin{aligned} x^m \circ x^n &= \underbrace{x \circ x \circ \cdots \circ x}_m \circ \underbrace{x \circ x \circ \cdots \circ x}_n \\ &= \underbrace{x \circ x \circ \cdots \circ x}_{m+n} \\ &= x^{m+n}. \end{aligned}$$

(b) We have

$$\begin{aligned} (x^m)^n &= \underbrace{x^m \circ x^m \circ \cdots \circ x^m}_n \\ &= \underbrace{\underbrace{x \circ x \circ \cdots \circ x}_m \circ \underbrace{x \circ x \circ \cdots \circ x}_m \circ \cdots \circ \underbrace{x \circ x \circ \cdots \circ x}_m}_n \\ &= \underbrace{x \circ x \circ \cdots \circ x}_{mn} \\ &= x^{mn}. \end{aligned}$$

- (c) The fact that $x^{-n} = (x^{-1})^n$, where n is a positive integer, is simply the definition of a negative power of a group element. You are asked to prove that $(x^n)^{-1} = (x^{-1})^n$ in the case $n = 2$ in the exercise below, and a proof for any positive integer n follows in a similar way. ■

Exercise B50

Let x be an element of a group (G, \circ) . Show that the inverse of x^2 is $(x^{-1})^2$.

Using index notation to denote repeated combinations of group elements works well for any group in which the binary operation is some kind of multiplication, and for any group in which the binary operation is function composition, such as a group of symmetries.

However, it is not appropriate for groups in which the binary operation is some kind of addition. For example, it would be confusing to denote the composite $x + x + x$ in the group $(\mathbb{R}, +)$ by x^3 . Instead, we denote it by $3x$, in the familiar way, and we refer to it as a **multiple** rather than a power.

So there are two types of notation that we can use for combinations of elements in groups: **multiplicative notation** and **additive notation**. These two types of notation also include different ways of representing other features of groups, such as the identity element and inverse elements. A summary is given in the box below.

Multiplicative notation and additive notation for groups

Feature	Multiplicative notation	Additive notation
Composite	$a \circ b$ or $a \times b$ or ab (or similar)	$a + b$ (or similar)
Identity	e or 1	0
Inverse	x^{-1}	$-x$
Power/multiple	x^n	nx

We always use multiplicative notation for groups in which the binary operation is some kind of multiplication, or function composition. We also use it for abstract groups, in which the binary operation is not specified as being of any particular type. A group for which we use multiplicative notation is called a **multiplicative** group.

We use additive notation for groups in which the binary operation is some kind of addition, such as addition of numbers, or modular addition. A group for which we use additive notation is called an **additive** group. Additive groups are always abelian, because addition is a commutative operation.

It is important to remember that a multiple in an additive group means the same as a power in a multiplicative group. For example, if x is an element of a multiplicative group (G, \circ) , then

$$x \circ x \circ x \circ x = x^4,$$

and if x is an element of an additive group $(G, +)$, then

$$x + x + x + x = 4x.$$

Similarly, if x is an element of a multiplicative group (G, \circ) , then

$$x^{-1} \circ x^{-1} \circ x^{-1} = (x^{-1})^3 = x^{-3},$$

and if x is an element of an additive group $(G, +)$, then

$$(-x) + (-x) + (-x) = 3(-x) = -3x.$$

Theorems, proofs and general discussions about group theory are normally expressed in multiplicative notation, both in this module and in mathematics in general. If you want to apply them to additive groups, then you have to translate them into additive notation. For example, here is Theorem B27 translated into additive notation. These laws should look familiar to you in this form too.

Theorem B28 Index laws (in additive notation)

Let x be an element of a group $(G, +)$, and let m and n be integers. The following laws hold.

- (a) $mx + nx = (m + n)x$
- (b) $n(mx) = (nm)x$
- (c) $-(nx) = (-n)x = n(-x)$

Exercise B51

Translate the following statements about elements x and y of a multiplicative group (G, \circ) into additive notation for elements x and y of an additive group $(G, +)$.

- (a) $x^0 = e$ (b) $x \circ x^{-1} = e$ (c) $x \circ x^2 = x^3$ (d) $(x^{-1})^{-1} = x$
- (e) $e \circ x = x$ (f) $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$

2.2 What is the order of a group element?

Now that we have the notation we need, let us look at what happens when we take an element of a group and repeatedly combine it with itself. In Exercise B49 you should have found that when you take the element a of the group $S(\square)$ and find the powers a, a^2, a^3, a^4 and so on, eventually you reach a power that is equal to the identity element e of the group. You should have found the same for the elements b and r of $S(\square)$. To enable us to describe situations like these, we make the definitions in the box below. Note that the word *order* in these definitions has a different meaning from the word *order* used to mean the size of a group. However, the two uses of the word are connected, as you will see in Section 3.

Definitions

Let x be an element of a group (G, \circ) .

If there is a positive integer n such that $x^n = e$, then the **order** of x is the *smallest* positive integer n such that $x^n = e$. We say that x has **finite order**.

If there is no positive integer n such that $x^n = e$, then x has **infinite order**.

For example, consider the following list of all the powers of the element a of the group $S(\square)$; the list includes the negative powers, and the zeroth power, as well as the positive powers. The powers are evaluated in the second line below (using Figure 7).

$$\begin{array}{cccccccccccccccc} \dots, & a^{-4}, & a^{-3}, & a^{-2}, & a^{-1}, & a^0, & a, & a^2, & a^3, & a^4, & a^5, & a^6, & a^7, & a^8, & a^9, & \dots \\ & & & & & \parallel & & & & & & & & & & & \\ \dots, & e, & a, & b, & c, & e, & a, & b, & c, & e, & a, & b, & c, & e, & a, & \dots \end{array}$$

The list shows that, for example, $a^{-4} = e$, $a^0 = e$, $a^4 = e$, and $a^8 = e$. The *smallest positive* integer n such that $a^n = e$ is 4, so a has order 4.

Similarly, consider the powers of 2 in the group (\mathbb{R}^*, \times) :

$$\begin{array}{cccccccccccccccc} \dots, & 2^{-3}, & 2^{-2}, & 2^{-1}, & 2^0, & 2, & 2^2, & 2^3, & 2^4, & 2^5, & 2^6, & 2^7, & \dots \\ & & & & \parallel & & & & & & & & & \\ \dots, & \frac{1}{8}, & \frac{1}{4}, & \frac{1}{2}, & 1, & 2, & 4, & 8, & 16, & 32, & 64, & 128, & \dots \end{array}$$

The identity element of (\mathbb{R}^*, \times) is 1, and there is no *positive* integer n such that $2^n = 1$, so 2 has infinite order in (\mathbb{R}^*, \times) .

Finally, consider the multiples of 2 in the additive group $(\mathbb{R}, +)$:

$$\begin{array}{cccccccccccccccc} \dots, & (-3) \times 2, & (-2) \times 2, & (-1) \times 2, & 0 \times 2, & 2, & 2 \times 2, & 3 \times 2, & \dots \\ & & & & \parallel & & & & & \\ \dots, & -6, & -4, & -2, & 0, & 2, & 4, & 6, & \dots \end{array}$$

The identity element of $(\mathbb{R}, +)$ is 0, and there is no *positive* integer n such that $n \times 2 = 0$, so 2 has infinite order in $(\mathbb{R}, +)$.

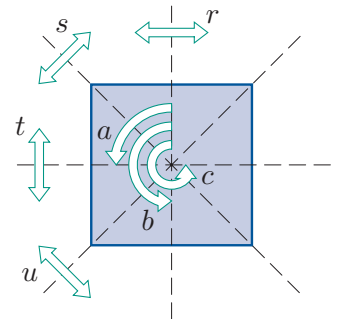
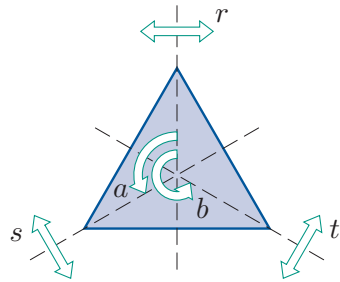


Figure 7 $S(\square)$

Figure 8 $S(\Delta)$

Worked Exercise B23

Find the order of the element a of $S(\Delta)$.

(The non-identity elements of $S(\Delta)$ are shown in Figure 8.)

Solution

We have

$$a^2 = a \circ a = b,$$

$$a^3 = a^2 \circ a = b \circ a = e.$$

Thus a in $S(\Delta)$ has order 3.

Alternatively, the smallest (positive) number of times that we need to apply a to bring the triangle back to its starting position is 3, so a has order 3.

Exercise B52

Find the orders of the following group elements.

- (a) The element c in $S(\square)$.
- (b) The element r in $S(\square)$.
- (c) The element 1 in $(\mathbb{Z}_6, +_6)$.
- (d) The element 2 in $(\mathbb{Z}_6, +_6)$.
- (e) The element 5 in (U_9, \times_9) .
- (f) The element 9 in (U_{10}, \times_{10}) .
- (g) The element 1 in $(\mathbb{Z}, +)$.
- (h) The element i in (\mathbb{C}^*, \times) .

Exercise B53

State the order of each element in the group $(\mathbb{Z}, +)$.

An element of a finite group always has finite order, as shown next.

Theorem B29

Let x be an element of a finite group (G, \circ) . Then x has finite order.

Proof Consider the list of consecutive powers of x :

$$\dots, x^{-4}, x^{-3}, x^{-2}, x^{-1}, x^0, x, x^2, x^3, x^4, \dots$$

The elements in this list cannot all be distinct, because they are all in G and there are only finitely many elements in G . So there must be integers s and t , with $s < t$, such that

$$x^s = x^t.$$

Composing each side of this equation with $(x^s)^{-1}$ on the right gives

$$x^s \circ (x^s)^{-1} = x^t \circ (x^s)^{-1}.$$

Simplifying (using the index laws on the right-hand side) gives

$$e = x^{t-s}.$$

Now $t - s$ is positive, since $s < t$. So there is a positive power of x that is equal to e , and hence x has finite order. ■

An element of an *infinite* group can have either finite order or infinite order. For example, in Exercise B52(h) you saw that the element i of the infinite group (\mathbb{C}^*, \times) has finite order, and you saw earlier that the element 2 of the infinite group (\mathbb{R}^*, \times) has infinite order.

The box below gives two simple results about the orders of group elements that are useful to remember.

Order of the identity and order of self-inverse elements

Let (G, \circ) be a group with identity element e .

- The identity element e has order 1.
- If the element x is self-inverse, and $x \neq e$, then x has order 2.

The first result holds because $e^1 = e$, so the smallest positive integer n such that $e^n = e$ is 1. The second result holds because if $x = x^{-1}$ then (by composing each side by x) we have $x^2 = e$. This tells us that, provided $x \neq e$, the smallest positive integer n such that $x^n = e$ is 2.

Here is another useful result about the orders of group elements.

Theorem B30

If x is an element of a group (G, \circ) , then either x and x^{-1} have the *same* finite order, or they both have infinite order.

Proof Let $x \in G$ and let the identity element of (G, \circ) be e .

First we show that for any integer n ,

$$x^n = e \quad \text{if and only if} \quad (x^{-1})^n = e. \quad (1)$$

To do this, let $n \in \mathbb{Z}$ and first suppose that

$$x^n = e.$$

Composing each side on the right by $(x^n)^{-1}$ gives

$$x^n \circ (x^n)^{-1} = e \circ (x^n)^{-1}.$$

Simplifying, and using the index laws on the right-hand side, gives

$$e = (x^{-1})^n.$$

So we have shown that

$$\text{if } x^n = e, \text{ then } (x^{-1})^n = e.$$

Since this statement holds if we replace x by any element of G , it holds if we replace x by x^{-1} . So, since $(x^{-1})^{-1} = x$, we have that

$$\text{if } (x^{-1})^n = e, \text{ then } x^n = e.$$

Thus statement (1) holds. This statement tells us that the values of n for which $x^n = e$ are exactly the same as the values of n for which $(x^{-1})^n = e$. It follows that either x and x^{-1} have the same finite order, or they both have infinite order. ■

Now that you have met the idea of the order of a group element, let us go back to looking at what happens when we repeatedly combine a group element with itself. Look again at the list of consecutive powers of the element a in the group $S(\square)$:

$$\begin{array}{cccccccccccccccc} \dots, & a^{-4}, & a^{-3}, & a^{-2}, & a^{-1}, & a^0, & a, & a^2, & a^3, & a^4, & a^5, & a^6, & a^7, & a^8, & a^9, & \dots \\ & & & & & \parallel & & & & & & & & & & & \\ \dots, & e, & a, & b, & c, & e, & a, & b, & c, & e, & a, & b, & c, & e, & a, & \dots \end{array}$$

The element a has order 4, and it looks as if a pattern of 4 distinct elements, namely e, a, b, c , keeps repeating indefinitely in the list of the powers of a .

In contrast, the element 2 in the group (\mathbb{R}^*, \times) has infinite order, and all the elements in its list of powers are *distinct*:

$$\begin{array}{cccccccccccccccc} \dots, & 2^{-3}, & 2^{-2}, & 2^{-1}, & a^0, & 2, & 2^2, & 2^3, & 2^4, & 2^5, & 2^6, & 2^7, & \dots \\ & & & & \parallel & & & & & & & & & \\ \dots, & \frac{1}{8}, & \frac{1}{4}, & \frac{1}{2}, & 1, & 2, & 4, & 8, & 16, & 32, & 64, & 128, & \dots \end{array}$$

In general, we have the following important result.

Theorem B31

Let x be an element of a group (G, \circ) .

(a) If x has finite order n , then the n powers

$$e, x, x^2, \dots, x^{n-1}$$

are distinct, and these elements repeat indefinitely every n powers in the list of consecutive powers of x .

(b) If x has infinite order, then all the powers of x are distinct.

Proof

- (a) Suppose that
- x
- has finite order
- n
- .

First, we prove by contradiction that the n powers

$$e, x, x^2, \dots, x^{n-1}$$

are distinct. Suppose that these powers are *not* distinct. Then

$$x^s = x^t$$

for some s and t with $0 \leq s < t \leq n - 1$. Composing each side of this equation on the right with $(x^s)^{-1}$, and arguing as in the proof of Theorem B29, we can deduce that

$$e = x^{t-s}.$$

But $0 < t - s < n$ (since $0 \leq s < t \leq n - 1$), so this contradicts the fact that n is the *smallest* positive integer such that $x^n = e$. It follows that the n powers listed above are all distinct.

Now we prove that the powers repeat every n elements. Consider any power of x of the form x^{kn} , where $k \in \mathbb{Z}$; that is, any power where the exponent is an integer multiple of the order n of x . We have

$$x^{kn} = (x^n)^k = e^k = e.$$

So, in the list of consecutive powers of x , the element e is repeated every n elements. Because each element in the list is obtained from the previous element by composing it with x , it follows that all the elements in the list repeat every n elements.

- (b) You are asked to prove this part in the next exercise.
-

Exercise B54

Use a contradiction argument to prove Theorem B31(b).

2.3 Finding the orders of group elements

When you want to find the orders of all the elements in some finite group, you can cut down your work by using some of the results that you met in the previous subsection: the identity element has order 1, all other self-inverse elements have order 2, and an element and its inverse always have the same order. This is illustrated in the worked exercise below.

Worked Exercise B24



Find the order of every element in each of the following groups.

- (a) $S(\square)$ (b) $(\mathbb{Z}_6, +_6)$

(See Figure 9 for a summary of the non-identity elements of $S(\square)$.)

Solution

- (a) The identity element e has order 1.

 The working needed to find the order of the element a of $S(\square)$ was part of what you were asked to do in Exercise B49. 

For the element a , we have

$$\begin{aligned} a^2 &= a \circ a = b, \\ a^3 &= a^2 \circ a = b \circ a = c, \\ a^4 &= a^3 \circ a = c \circ a = e. \end{aligned}$$



Thus a has order 4. Hence c , the inverse of a , also has order 4.

All the other elements of $S(\square)$ are self-inverse and hence have order 2.

In summary, the orders of the elements of $S(\square)$ are as follows.

Element	e	a	b	c	r	s	t	u
Order	1	4	2	4	2	2	2	2

- (b) The identity element 0 has order 1.

 You found the orders of the elements 1 and 2 of $(\mathbb{Z}_6, +_6)$ in Exercise B52. 

For the element 1, we have

$$\begin{aligned} 1 +_6 1 &= 2 \\ 1 +_6 1 +_6 1 &= 3 \\ 1 +_6 1 +_6 1 +_6 1 &= 4 \\ 1 +_6 1 +_6 1 +_6 1 +_6 1 &= 5 \\ 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 &= 0 \end{aligned}$$

Thus 1 has order 6. Hence 5, the inverse of 1, also has order 6.

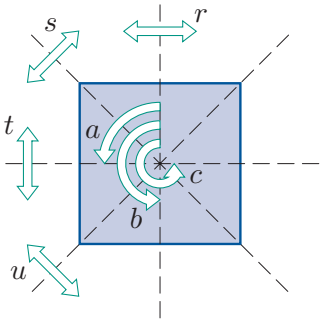


Figure 9 $S(\square)$

For the element 2, we have

$$2 +_6 2 = 4$$

$$2 +_6 2 +_6 2 = 0$$

Thus 2 has order 3. Hence 4, the inverse of 2, also has order 3.

Finally, the element 3 is self-inverse, so it has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_6, +_6)$ are as follows.

Element	0	1	2	3	4	5
Order	1	6	3	2	3	6

Exercise B55

Find the order of every element in each of the following groups.

- (a) $S(\triangle)$ (b) $S(\square)$ (c) $(\mathbb{Z}_5^*, \times_5)$ (d) $(\mathbb{Z}_8, +_8)$

(The non-identity elements of $S(\triangle)$ and $S(\square)$ are shown in Figures 10 and 11.)

It is useful to think of the powers of a group element of finite order as forming a cycle. Theorem B31(a) tells us that, if we take a group element x of finite order n , and find its powers x^2, x^3 , and so on, then successive powers cycle indefinitely through n distinct group elements, as illustrated in Figure 12. Once we reach x^{n-1} , the next element is e , and then the cycle repeats.

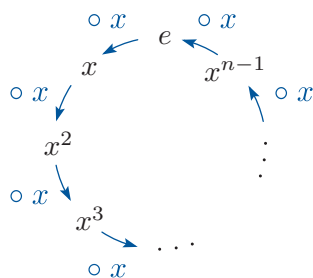


Figure 12 The effect of repeatedly composing a group element x of order n with itself

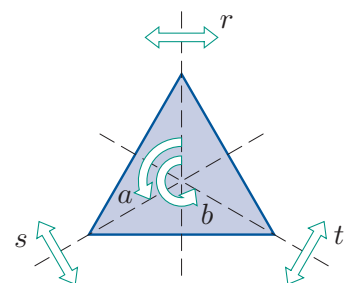


Figure 10 $S(\triangle)$

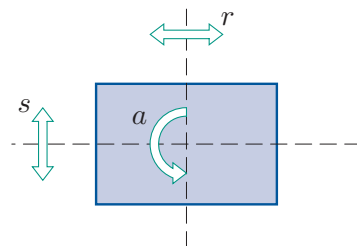


Figure 11 $S(\square)$

For example, Figure 13(a) shows what happens when we find powers of the element a in $S(\square)$, and Figure 13(b) shows what happens when we find multiples of the element 1 in $(\mathbb{Z}_6, +_6)$. (The non-identity elements of $S(\square)$ are shown again in Figure 14.)

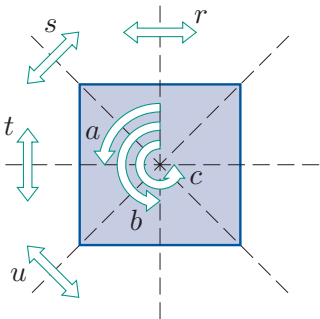


Figure 14 $S(\square)$

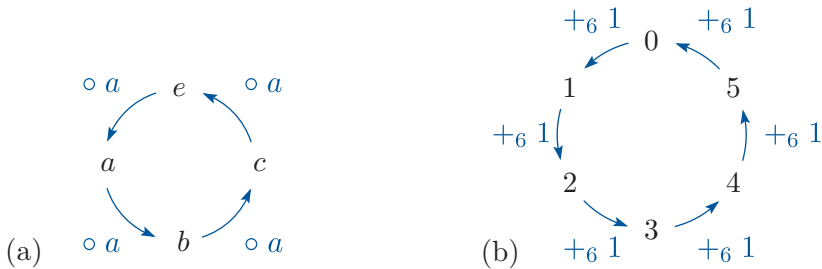


Figure 13 (a) The cycle of powers of the element a in $S(\square)$ (b) the cycle of multiples of the element 1 in $(\mathbb{Z}_6, +_6)$

You can use cycles like those in Figure 13 to find the powers of any of the group elements that appear in the cycle, and this can help you cut down your work further when you want to find the orders of group elements.

For example, consider the cycle of powers of the element a of $S(\square)$ in Figure 13(a). Moving one place round the cycle corresponds to composing by a . So moving one place round the cycle *in the reverse direction*, as shown by the inner arrows in Figure 15(a), corresponds to composing by a^{-1} , that is, composing by c . So if we start from e and go round the cycle in the reverse direction, then we will obtain the powers $e, c, c^2, c^3, c^4, \dots$. Hence this list of powers evaluates to $e, c, c^2, c^3, c^4, \dots$. This shows in particular that c has order 4, as found in Worked Exercise B24, which is as expected, since a group element and its inverse have the same order.

Similarly, moving *two* places round this cycle *in the original direction*, as shown by the inner arrows in Figure 15(b), corresponds to composing by a^2 , that is, composing by b . So if we start from e and go round the cycle two places at a time in the direction of the arrows, then we will obtain the powers $e, b, b^2, b^3, b^4, \dots$. Hence this list of powers evaluates to e, b, e, b, e, \dots , which shows that b has order 2, as also found in Worked Exercise B24.

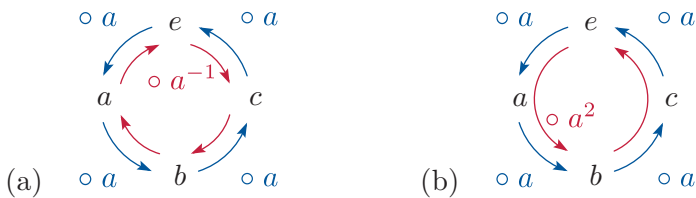


Figure 15 Moving round the cycle of powers of a in $S(\square)$ (a) in the reverse direction (b) in the original direction, two places at a time

Notice that the element that appears immediately before the identity element e in the cycle of powers of a in $S(\square)$ (shown in Figure 13(a)) is c , the inverse of a . This is because multiplying this element by a gives e . In general, we have the following fact.

Let x be a group element of finite order. In the cycle of powers of x , the element that appears immediately before the identity element is the inverse of x .

Exercise B56

- (a) Write down the elements of the group (U_{20}, \times_{20}) , and use any method to find the order of every element of this group.
- (b) Use any method to find the order of every element of the group $(\mathbb{Z}_{12}, +_{12})$.

3 Cyclic subgroups and cyclic groups

The ideas that you met in the previous section give us a way of finding some of the subgroups of a group, and can also give us an insight into the structure of some groups, as you will see in this section.

3.1 The subgroup generated by an element

In this subsection we consider the set formed by all the powers of a group element.

Definition

Let x be an element of a group (G, \circ) . The set of all powers of x is called the subset of G **generated** by x , and denoted by $\langle x \rangle$. That is,

$$\langle x \rangle = \{x^k : k \in \mathbb{Z}\}.$$

In additive notation, if x is an element of a group $(G, +)$, then the subset of G generated by x is the set of all multiples of x :

$$\langle x \rangle = \{kx : k \in \mathbb{Z}\}.$$

A subset of a group generated by an element may be either finite or infinite, as illustrated by the worked exercise below.

Worked Exercise B25

Find the following generated subsets.

- The subset $\langle a \rangle$ of the group $S(\square)$.
- The subset $\langle 2 \rangle$ of the group (\mathbb{R}, \times) .
- The subset $\langle 2 \rangle$ of the group $(\mathbb{Z}_6, +_6)$.

Solution

- We saw earlier (near the start of Subsection 2.2) that the list of consecutive powers of a in $S(\square)$ is

$$\dots, e, a, b, c, e, a, b, c, e, a, b, c, \dots$$

Hence

$$\langle a \rangle = \{e, a, b, c\}.$$

- In (\mathbb{R}, \times) , we have

$$\begin{aligned} \langle 2 \rangle &= \{2^k : k \in \mathbb{Z}\} \\ &= \{\dots, 2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, 2^4, \dots\} \\ &= \{\dots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \dots\}. \end{aligned}$$

- In $(\mathbb{Z}_6, +_6)$, the list of consecutive multiples of 2 is

$$\dots, 0, 2, 4, 0, 2, 4, 0, 2, 4, \dots$$

Hence

$$\langle 2 \rangle = \{0, 2, 4\}.$$

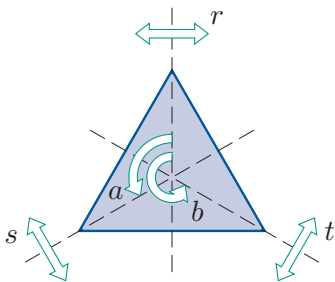


Figure 16 $S(\Delta)$

Exercise B57

Find the following generated subsets.

- The subset $\langle a \rangle$ of the group $S(\Delta)$.
- The subset $\langle 3 \rangle$ of the group $(\mathbb{Z}_7^*, \times_7)$.
- The subset $\langle 2 \rangle$ of the group $(\mathbb{Z}, +)$.

A reminder of the non-identity elements of $S(\Delta)$ is given in Figure 16.

The generated subsets found in Worked Exercise B25 and Exercise B57 are in fact all *subgroups* of the groups mentioned. This follows from the following theorem, which applies to both finite and infinite groups.

Theorem B32

Let x be an element of a group (G, \circ) . Then $(\langle x \rangle, \circ)$ is a subgroup of (G, \circ) .

Proof We check that the three subgroup properties hold.

SG1 Closure Let g and h be elements of $\langle x \rangle$. Then $g = x^s$ and $h = x^t$ for some integers s and t . So

$$g \circ h = x^s \circ x^t = x^{s+t}.$$

Thus $g \circ h$ can be written as a power of x , so $g \circ h \in \langle x \rangle$.

SG2 Identity The identity element e of (G, \circ) can be written as $e = x^0$, so it is in $\langle x \rangle$.

SG3 Inverses Let g be any element of $\langle x \rangle$. Then $g = x^s$ for some integer s . Now

$$\begin{aligned} g^{-1} &= (x^s)^{-1} \\ &= x^{-s} \quad (\text{by one of the index laws}). \end{aligned}$$

Thus g^{-1} can be written as a power of x , so $g^{-1} \in \langle x \rangle$.

Since all three subgroup properties hold, $(\langle x \rangle, \circ)$ is a subgroup of (G, \circ) . ■

If x is an element of a group (G, \circ) , then we usually denote the subgroup $(\langle x \rangle, \circ)$ of G simply by $\langle x \rangle$, because the binary operation is clear from the context. We call this subgroup the **cyclic subgroup** of G **generated** by x . We also say that x is a **generator** of $\langle x \rangle$.

The order of the subgroup $\langle x \rangle$ (that is, the number of elements that it contains) is determined by the order of the element x , as set out in the next theorem. This theorem provides a connection between the two uses of the word ‘order’ in group theory, namely for the order of a group element (the smallest positive power or multiple of the element that equals the identity) and for the order of a group (the number of elements in the group).

Theorem B33

Let x be an element of a group.

- (a) If x has finite order n , then the subgroup $\langle x \rangle$ has order n .

In multiplicative notation,

$$\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}.$$

In additive notation,

$$\langle x \rangle = \{0, x, 2x, \dots, (n-1)x\}.$$

- (b) If x has infinite order, then the subgroup $\langle x \rangle$ has infinite order.

In multiplicative notation,

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}.$$

In additive notation,

$$\langle x \rangle = \{\dots, -2x, -x, 0, x, 2x, \dots\}.$$

Proof This theorem follows immediately from Theorem B31. ■

As an illustration of Theorem B33, consider the element a of $S(\square)$. It has order 4, and the cyclic subgroup $\langle a \rangle = \{e, a, b, c\}$ that it generates has order 4 (that is, it has 4 elements). As another illustration, consider the element 2 of $(\mathbb{Z}, +)$. It has infinite order, and it generates a cyclic subgroup of infinite order, as you saw in Exercise B57(c).

Note that the subgroup of $(\mathbb{Z}, +)$ generated by 2 is the subgroup $(2\mathbb{Z}, +)$:

$$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = 2\mathbb{Z}.$$

In general, for any integer n , the subgroup of $(\mathbb{Z}, +)$ generated by n is the subgroup $(n\mathbb{Z}, +)$.

The following results about cyclic subgroups follow from the simple results about the order of a group element that you met in Subsection 2.2 (Theorem B30 and the preceding box).

Some special cyclic subgroups

Let (G, \circ) be a group with identity element e , and let $x \in G$.

- $\langle e \rangle = \{e\}$.
- If x is self-inverse and $x \neq e$, then $\langle x \rangle = \{e, x\}$.
- $\langle x^{-1} \rangle = \langle x \rangle$.

Proof The first two results here follow from the properties in the box that precedes Theorem B30. For the third result, x^{-1} is an element of the subgroup generated by x , so $\langle x^{-1} \rangle$ is a subgroup of $\langle x \rangle$. Also, $x = (x^{-1})^{-1}$

is an element of the subgroup generated by x^{-1} , so $\langle x \rangle$ is a subgroup of $\langle x^{-1} \rangle$. It follows that $\langle x^{-1} \rangle$ and $\langle x \rangle$ are equal. ■

When you want to find the cyclic subgroup generated by each element in some group, the working that you need to carry out is essentially the same as the working you need to carry out to find the orders of all the elements in the group. This is illustrated in the next worked exercise. You can cut down the work needed by using the results in the box above, and by using the techniques that you met in Subsection 2.3.

Worked Exercise B26

Find the cyclic subgroup generated by each element in the following groups.

- (a) $S(\square)$ (see Figure 17) (b) $(\mathbb{Z}_6, +_6)$

Solution

- (a) Since e is the identity element in $S(\square)$, we have

$$\langle e \rangle = \{e\}.$$

💡 To find the cyclic subgroup $\langle a \rangle$, find the consecutive powers of a , starting at the identity element e and stopping when e is reached again. 💡

The powers of a are

$$a^0 = e, \quad a^1 = a, \quad a^2 = b, \quad a^3 = c, \quad a^4 = e, \quad \dots$$

So

$$\langle a \rangle = \{e, a, b, c\}.$$

💡 Use the fact that an element and its inverse generate the same cyclic subgroup. 💡

The element c is the inverse of a , so

$$\langle c \rangle = \{e, a, b, c\}.$$

The remaining elements are all self-inverse, so

$$\langle b \rangle = \{e, b\},$$

$$\langle r \rangle = \{e, r\},$$

$$\langle s \rangle = \{e, s\},$$

$$\langle t \rangle = \{e, t\},$$

$$\langle u \rangle = \{e, u\}.$$

💡 As you would expect from Theorem B33, the orders of the cyclic subgroups of $S(\square)$ agree with the orders of their generators, which we found in Worked Exercise B24. 💡

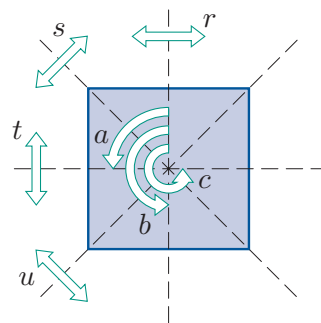


Figure 17 $S(\square)$

(b) Since 0 is the identity element in $(\mathbb{Z}_6, +_6)$, we have

$$\langle 0 \rangle = \{0\}.$$

💡 To find the cyclic subgroup $\langle 1 \rangle$, find the consecutive multiples of 1, starting at the identity element 0 and stopping when 0 is reached again. Of course, finding consecutive multiples of 1 is trivial! 🧠

The multiples of 1 in $(\mathbb{Z}_6, +_6)$ are

$$\dots, 0, 1, 2, 3, 4, 5, 0, \dots,$$

and 5 is the inverse of 1, so

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\},$$

$$\langle 5 \rangle = \{0, 1, 2, 3, 4, 5\}.$$

💡 To find the cyclic subgroup $\langle 2 \rangle$, find the consecutive multiples of 2, starting at the identity element 0 and stopping when 0 is reached again. 🧠

The multiples of 2 in $(\mathbb{Z}_6, +_6)$ are

$$\dots, 0, 2, 4, 0, \dots,$$

and 4 is the inverse of 2, so

$$\langle 2 \rangle = \{0, 2, 4\},$$

$$\langle 4 \rangle = \{0, 2, 4\}.$$

Finally, 3 is self-inverse, so

$$\langle 3 \rangle = \{0, 3\}.$$

💡 Again, the orders of the cyclic subgroups agree with the orders of their generators, as expected from Theorem B33. 🧠

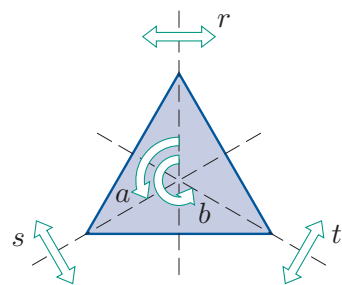


Figure 18 $S(\triangle)$

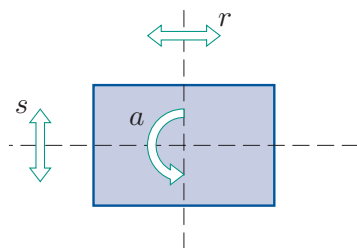


Figure 19 $S(\square)$

Exercise B58

Find the cyclic subgroup generated by each element in each of the following groups.

- (a) $S(\triangle)$ (b) $S(\square)$ (c) $(\mathbb{Z}_5^*, \times_5)$ (d) $(\mathbb{Z}_8, +_8)$

(Your working for Exercise B55 should be helpful. The non-identity elements of $S(\triangle)$ and $S(\square)$ are shown in Figures 18 and 19.)

Worked Exercise B26 and Exercise B58 illustrate that one way to find some subgroups of a group is to find its cyclic subgroups.

Notice, however, that different elements of the group can generate the same cyclic subgroup. For example, in $S(\square)$, the elements a and c both generate the subgroup $\{e, a, b, c\}$.

Note also that a group can have subgroups that are not cyclic subgroups. For example, $\{e, b, r, t\}$ is a subgroup of $S(\square)$, as you saw in Worked Exercise B19, but it is not generated by any of the elements of $S(\square)$, as you can see from the solution to Worked Exercise B26(a).

Cyclic subgroups of $S(\bigcirc)$

To end this subsection, let us find some cyclic subgroups of $S(\bigcirc)$, the symmetry group of the disc.

Remember from Unit B1 that the symmetries of the disc are:

- r_θ : rotation through an angle θ about the centre, for $\theta \in [0, 2\pi)$
- q_θ : reflection in the line through the centre at an angle θ to the horizontal (measured anticlockwise), for $\theta \in [0, \pi)$.

So

$$S(\bigcirc) = \{r_\theta : \theta \in [0, 2\pi)\} \cup \{q_\theta : \theta \in [0, \pi)\}.$$

The identity element of the group $S(\bigcirc)$ is r_0 .

Any reflection q_θ is self-inverse, as illustrated in Figure 20, so it has order 2 and generates a cyclic subgroup

$$\langle q_\theta \rangle = \{r_0, q_\theta\}$$

of order 2.

The situation with the rotations in $S(\bigcirc)$ is more complicated. First, let us find a formula for a power of a rotation. If we take a particular rotation r_θ and apply it k times, then the effect is the same as that of applying the rotation $r_{k\theta}$. That is,

$$r_\theta^k = r_{k\theta}.$$

Of course, the angle $k\theta$ may not lie in the interval $[0, 2\pi)$, but $r_{k\theta}$ is equivalent to a rotation through an angle that does lie in this interval.

Some of the rotations in $S(\bigcirc)$ have finite order. For example, for the rotation $r_{2\pi/5}$, the five powers

$$\begin{aligned} r_{2\pi/5}^0 &= r_0, \\ r_{2\pi/5}^1 &= r_{2\pi/5}, \\ r_{2\pi/5}^2 &= r_{4\pi/5}, \\ r_{2\pi/5}^3 &= r_{6\pi/5}, \\ r_{2\pi/5}^4 &= r_{8\pi/5} \end{aligned}$$

are all distinct, as illustrated in Figure 21, and the next power is

$$r_{2\pi/5}^5 = r_{10\pi/5} = r_{2\pi} = r_0,$$

so the powers start repeating. So this rotation has order 5 and generates the following cyclic subgroup of order 5:

$$\langle r_{2\pi/5} \rangle = \{r_0, r_{2\pi/5}, r_{4\pi/5}, r_{6\pi/5}, r_{8\pi/5}\}.$$

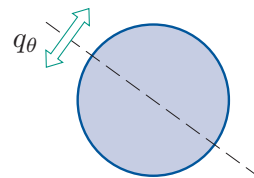


Figure 20 A reflection q_θ

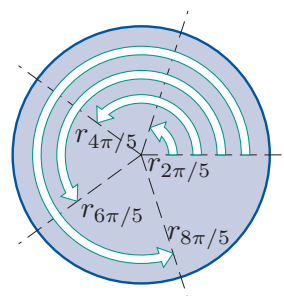


Figure 21 Powers of $r_{2\pi/5}$

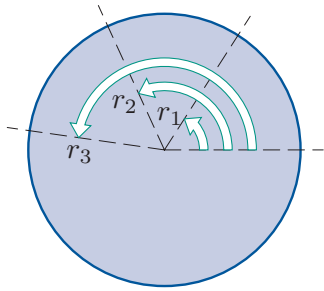


Figure 22 Some powers of r_1

Other rotations have infinite order. For example, consider r_1 , the rotation through one radian, which is just over 57° , as illustrated in Figure 22. We have

$$r_1^2 = r_{2 \times 1} = r_2,$$

$$r_1^3 = r_{3 \times 1} = r_3,$$

and so on. No power of r_1 is equal to the identity symmetry r_0 . To see this, we can use the fact that the k th power of r_1 is given by

$$r_1^k = r_{k \times 1} = r_k.$$

So if there *were* an integer k such that $r_1^k = r_0$, then k would be a multiple of 2π , say $k = 2s\pi$ where s is an integer, and this equation gives $\pi = k/(2s)$, which is impossible as π is irrational. So r_1 generates a cyclic subgroup of infinite order.

Exercise B59

Find the order of each of the following cyclic subgroups of $S(\circ)$.

- (a) $\langle r_{\pi/4} \rangle$ (b) $\langle r_{\pi/3} \rangle$ (c) $\langle r_{2\pi/7} \rangle$ (d) $\langle r_2 \rangle$

3.2 Cyclic groups

In Worked Exercise B26 we found all the cyclic subgroups of the groups $S(\square)$ and $(\mathbb{Z}_6, +_6)$, as follows.

Cyclic subgroups of $S(\square)$ Cyclic subgroups of $(\mathbb{Z}_6, +_6)$

$$\langle e \rangle = \{e\}$$

$$\langle a \rangle = \{e, a, b, c\}$$

$$\langle b \rangle = \{e, b\}$$

$$\langle c \rangle = \{e, a, b, c\}$$

$$\langle r \rangle = \{e, r\}$$

$$\langle s \rangle = \{e, s\}$$

$$\langle t \rangle = \{e, t\}$$

$$\langle u \rangle = \{e, u\}$$

$$\langle 0 \rangle = \{0\}$$

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$$

$$\langle 2 \rangle = \{0, 2, 4\}$$

$$\langle 3 \rangle = \{0, 3\}$$

$$\langle 4 \rangle = \{0, 2, 4\}$$

$$\langle 5 \rangle = \{0, 1, 2, 3, 4, 5\}$$

Notice that $(\mathbb{Z}_6, +_6)$ contains two elements that each generate the whole group:

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6,$$

$$\langle 5 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6.$$

In contrast, none of the elements of the group $S(\square)$ generates the whole group $S(\square) = \{e, a, b, c, r, s, t, u\}$: each element generates only a proper subgroup.

We make the following definitions.

Definitions

Let G be a group. If there is an element $x \in G$ such that $G = \langle x \rangle$, then G is a **cyclic group**.

If there is no such element, then G is **non-cyclic**.

So $(\mathbb{Z}_6, +_6)$ is a cyclic group, whereas $S(\square)$ is non-cyclic.

The following theorem follows immediately from the fact that a group element of order n generates a cyclic subgroup of order n (Theorem B33(a)).

Theorem B34

Let G be a finite group of order n . Then G is cyclic if and only if G contains an element of order n .

So $(\mathbb{Z}_6, +_6)$ is cyclic because it has order 6 and contains an element of order 6 (namely 1 or 5). On the other hand, $S(\square)$ is non-cyclic because it has order 8 but contains no element of order 8. When you want to show that a group is cyclic, it is sometimes more efficient to use Theorem B34 rather than the definition of a cyclic group.

Exercise B60

Determine which of the following groups are cyclic. (You were asked to find the order of each element of these groups in Exercise B55.)

- (a) $S(\triangle)$ (b) $S(\square)$ (c) $(\mathbb{Z}_5^*, \times_5)$ (d) $(\mathbb{Z}_8, +_8)$

The definitions of cyclic and non-cyclic groups apply to both finite and infinite groups. An example of an infinite cyclic group is $(\mathbb{Z}, +)$, because in this group

$$\begin{aligned}\langle 1 \rangle &= \{k \times 1 : k \in \mathbb{Z}\} \\ &= \{\dots, -2, -1, 0, 1, 2, \dots\} \\ &= \mathbb{Z}.\end{aligned}$$

Since $(\mathbb{Z}, +)$ is generated by 1, it is also generated by -1 , the inverse of 1:

$$\begin{aligned}\langle -1 \rangle &= \{k \times (-1) : k \in \mathbb{Z}\} \\ &= \{\dots, 2, 1, 0, -1, -2, \dots\} \\ &= \{\dots, -2, -1, 0, 1, 2, \dots\} \\ &= \mathbb{Z}.\end{aligned}$$

An example of an infinite group that is not cyclic is (\mathbb{R}^*, \times) . One way to see that this group is non-cyclic is to use a contradiction argument, as follows. Suppose that (\mathbb{R}^*, \times) is cyclic, with generator x . Then, since $-1 \in \mathbb{R}^*$, there is a non-zero integer k such that

$$x^k = -1.$$

It follows that

$$x^k \times x^k = (-1) \times (-1),$$

that is

$$x^{2k} = 1. \tag{2}$$

It follows from this equation that

$$(x^{2k})^{-1} = 1^{-1},$$

that is,

$$x^{-2k} = 1. \tag{3}$$

Since one of $2k$ and $-2k$ must be positive, equations (2) and (3) tell us that there is a positive integer n such that $x^n = 1$. Hence x has finite order. Therefore x does not generate \mathbb{R}^* , which is a contradiction.

The theorem below gives a simple property of cyclic groups. You are asked to try to prove it in the next exercise.

Theorem B35

Every cyclic group is abelian.

Exercise B61

Show that if (G, \circ) is a cyclic group, then (G, \circ) is abelian.

Hint: Suppose that (G, \circ) is generated by a . Then every element of G can be expressed as a power of a .

The next theorem gives a less obvious property of cyclic groups. It applies to both finite and infinite groups. The proof of this theorem is quite complicated; if you are interested in it, and have plenty of time, then take the time to read it and understand it, but do not worry about skipping it otherwise. At this stage you are likely to learn more from simpler proofs in group theory.

Theorem B36

Every subgroup of a cyclic group is cyclic.

Proof Let (G, \circ) be a cyclic group, generated by a , and let H be a subgroup of (G, \circ) .

If H is the trivial subgroup, then it is cyclic (generated by the identity element). So now suppose that H is not the trivial subgroup. All the elements of H can be expressed as powers of a (because H is a subset of G), and hence H must contain at least one element that can be expressed as a^k where k is *positive*, because H is a subgroup of G and therefore if $a^k \in H$ then also $(a^k)^{-1} = a^{-k} \in H$. Let m be the *smallest* positive integer such that a^m is in H . We will show that a^m generates H .

To do this, we have to show that every element of H can be expressed as a power of a^m . So let h be an element of H . Then $h = a^k$ for some integer k . The Division Theorem, which you met in Unit A2 *Number systems* gives

$$k = qm + r,$$

where q and r are integers, and $0 \leq r < m$. Thus

$$r = k - qm,$$

so, by the index laws for group elements,

$$a^r = a^{k-qm} = a^k \circ (a^m)^{-q}.$$

Now both a^k and a^m are elements of H , and H is a group under \circ , so it follows from the equation above that a^r is in H . Hence, since $0 \leq r < m$ and m is the *smallest* positive integer such that a^m is in H , we must have $r = 0$. Thus $k = qm$, and so

$$h = a^k = (a^m)^q.$$

This shows that h can be expressed as a power of a^m , which completes the proof. ■

Earlier in this unit you met some methods for finding some of the subgroups of a symmetry group. In general, finding *all* the subgroups of a finite group is a tricky and time-consuming task. Theorem B36 tells us that the task is much simpler if the group is cyclic: we just have to find all its distinct *cyclic* subgroups. This is illustrated below.

Worked Exercise B27

Find all the subgroups of the group $(\mathbb{Z}_6, +_6)$, writing down a list in which each subgroup appears just once.

Solution

The cyclic subgroups of the group $(\mathbb{Z}_6, +_6)$ (as found in Worked Exercise B26) are as follows.

💡 Remember that an element and its inverse generate the same cyclic subgroup. 💡

$$\begin{aligned}\langle 0 \rangle &= \{0\}, \\ \langle 1 \rangle &= \langle 5 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6, \\ \langle 2 \rangle &= \langle 4 \rangle = \{0, 2, 4\}, \\ \langle 3 \rangle &= \{0, 3\}.\end{aligned}$$

Since $\langle 1 \rangle = \mathbb{Z}_6$, the group $(\mathbb{Z}_6, +_6)$ is cyclic, and hence all its subgroups are cyclic.

So all the subgroups of $(\mathbb{Z}_6, +_6)$ are included in the list above.

So the subgroups of $(\mathbb{Z}_6, +_6)$ are:

$$\{0\}, \quad \{0, 2, 4\}, \quad \{0, 3\}, \quad \mathbb{Z}_6.$$

Exercise B62

You saw in Exercise B60 that the two groups below are cyclic, and you were asked to find all their cyclic subgroups in Exercise B58. Find all the subgroups of each group, writing down a list in which each subgroup appears just once.

$$(a) (\mathbb{Z}_5^*, \times_5) \quad (b) (\mathbb{Z}_8, +_8)$$

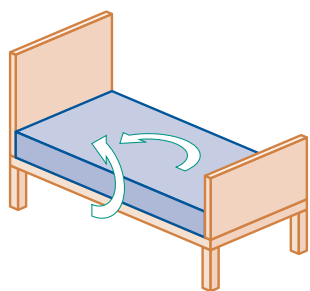


Figure 23 Turning a mattress

Group theory and mattress turning

There is a connection between the theory of cyclic groups and the question of how you turn your mattress. Some mattresses need to be turned, every few months, such that the turning includes both head to foot rotating, and top to bottom flipping, as illustrated in Figure 23. There are four possible positions in which such a mattress can be placed on the bed, so the group of direct symmetries of the mattress (when the mattress is regarded as a perfect cuboid, of course) has order 4. It would be nice if there were a particular mattress turning move, such that if you used this move every time you turned the mattress, then the mattress would cycle through its four possible positions in turn. Unfortunately, there is no such move – this is because the group of direct symmetries of the mattress is not cyclic!

Some more modern mattresses need to be rotated head to foot only, and should not be flipped over. So they have only two possible positions; these correspond to a subgroup of order 2 of the group of direct symmetries of the mattress. Every group of order 2 is cyclic (generated by the single element that is not the identity element), so with such a mattress you *can* make the same move each time, and have the mattress cycle through its two possible positions.

3.3 Cyclic groups from modular arithmetic

In this subsection we focus on cyclic groups that arise from modular arithmetic.

Additive cyclic groups from modular arithmetic

In the previous subsection you saw that the additive groups $(\mathbb{Z}_6, +_6)$ and $(\mathbb{Z}_8, +_8)$ are cyclic groups. Each of these cyclic groups is generated by the integer 1, as shown in Figure 24.

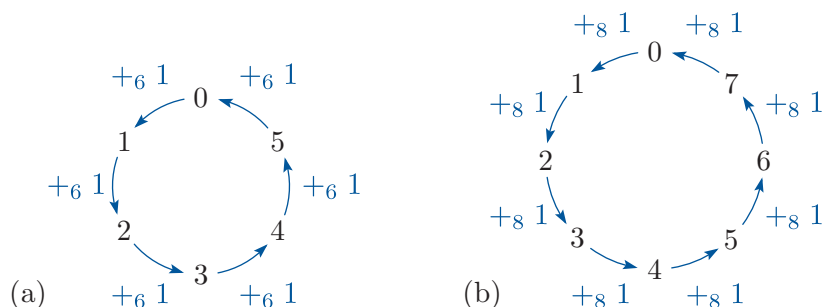


Figure 24 The cycle of multiples of 1 in (a) $(\mathbb{Z}_6, +_6)$ (b) $(\mathbb{Z}_8, +_8)$

In general, for any positive integer n , the cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$ contains each element of \mathbb{Z}_n , and hence generates the whole group $(\mathbb{Z}_n, +_n)$, as shown in Figure 25.

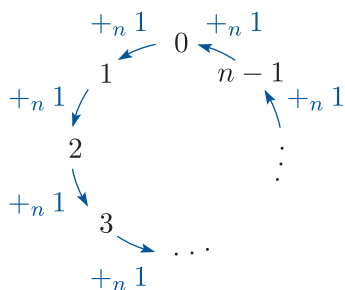


Figure 25 The cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$

So we can state the following result.

Theorem B37

For each integer $n \geq 2$, the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n . It is generated by the integer 1.

In general the integer 1 is not the only generator of the cyclic group $(\mathbb{Z}_n, +_n)$. The inverse of 1 (which is $n-1$, since $1 +_n (n-1) = 0$) also generates the group, as you know from Subsection 3.1, and usually some other integers do too, as illustrated in the next exercise.

Exercise B63

By looking back at your answer (or the solution) to Exercise B58(d), write down all the generators of the cyclic group $(\mathbb{Z}_8, +_8)$.

In Subsection 3.4 you will meet a result that tells you exactly which elements of \mathbb{Z}_n are generators of the cyclic group $(\mathbb{Z}_n, +_n)$, for any $n \geq 2$.

Multiplicative cyclic groups from modular arithmetic

In Theorem B9 of Unit B1 you saw that for all integers $n \geq 2$, the set U_n of integers in \mathbb{Z}_n coprime to n is a group under \times_n . The next two activities demonstrate that the group (U_n, \times_n) may or may not be cyclic.

Exercise B64

- (a) Write down the elements of the group (U_{18}, \times_{18}) .
- (b) Find all the cyclic subgroups of this group.
- (c) Deduce that (U_{18}, \times_{18}) is cyclic, and list all its generators.

Exercise B65

Use the solution to Exercise B56(a) to show that (U_{20}, \times_{20}) is not a cyclic group.

Since the group (U_{18}, \times_{18}) is cyclic it is straightforward to write down all of its subgroups, as they must all be cyclic, by Theorem B36. In contrast, the non-cyclic group (U_{20}, \times_{20}) may have some subgroups that are not cyclic.

Exercise B66

Using your answer to Exercise B64, write down all the subgroups of the group (U_{18}, \times_{18}) , giving a list in which each subgroup appears just once.

Exercise B67

Show that $(\{1, 9, 11, 19\}, \times_{20})$ is a subgroup of (U_{20}, \times_{20}) , but that it is not a cyclic subgroup.

3.4 The group $(\mathbb{Z}_n, +_n)$

In this subsection we will look more closely at the additive cyclic group $(\mathbb{Z}_n, +_n)$, $n \geq 2$. In particular we will look at how we can determine the orders of its elements, and how we can efficiently find its subgroups.

Orders of elements of $(\mathbb{Z}_n, +_n)$

We have found the orders of all the elements in several of the groups $(\mathbb{Z}_n, +_n)$, as follows.

$(\mathbb{Z}_6, +_6)$	Element	0	1	2	3	4	5
	Order	1	6	3	2	3	6

$(\mathbb{Z}_8, +_8)$	Element	0	1	2	3	4	5	6	7
	Order	1	8	4	8	2	8	4	8

$(\mathbb{Z}_{12}, +_{12})$	Element	0	1	2	3	4	5	6	7	8	9	10	11
	Order	1	12	6	4	3	12	2	12	3	4	6	12

These results were obtained in Worked Exercise B24, Exercise B55(d) and Exercise B56(b), respectively. In the next exercise you are asked to find the orders of the elements in another group $(\mathbb{Z}_n, +_n)$. In this case the value of n is prime.

Exercise B68

Find the order of each element of the group $(\mathbb{Z}_5, +_5)$.

The order of an integer m in a cyclic group $(\mathbb{Z}_n, +_n)$ must be related to the integers m and n – but how? The examples above and the solution to Exercise B68 seem to suggest that the order of the integer m in $(\mathbb{Z}_n, +_n)$ is always a factor of n , but it is hard to spot a pattern that might suggest what the exact relationship is. In fact, the relationship is as follows.

Theorem B38 Order of an element of $(\mathbb{Z}_n, +_n)$

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. Then m has order n/d , where d is the highest common factor (HCF) of m and n .

This theorem is simple to state, and it has a number of important consequences, but unfortunately it is quite complicated to prove. A proof is provided at the end of this subsection for those who are interested and have plenty of time, but you can skip it if you prefer.

Notice that the theorem tells us how to work out the order of each *non-zero* integer in any group $(\mathbb{Z}_n, +_n)$. However, we already know that the order of the integer 0 in $(\mathbb{Z}_n, +_n)$ is 1, since 0 is the identity element in $(\mathbb{Z}_n, +_n)$.

Worked Exercise B28

Use Theorem B38 to find the order of the integer 8 in $(\mathbb{Z}_{12}, +_{12})$.

Solution

The HCF of 8 and 12 is 4, so the order of 8 in $(\mathbb{Z}_{12}, +_{12})$ is $12/4 = 3$.

Exercise B69

Using Theorem B38, determine the order of each integer in each of the following groups. Check that your answer to part (a) agrees with the table of orders of elements of $(\mathbb{Z}_6, +_6)$ at the start of this subsection, and that your answer to part (b) agrees with your answer to Exercise B68.

- (a) $(\mathbb{Z}_6, +_6)$ (b) $(\mathbb{Z}_5, +_5)$

In Exercise B69(b) (and also in Exercise B68 earlier) you should have found that the order of every non-zero integer in $(\mathbb{Z}_5, +_5)$ is 5. This is an instance of the following corollary to Theorem B38.

Corollary B39

Let m be a non-zero element of the group $(\mathbb{Z}_p, +_p)$, where p is prime. Then m has order p .

Proof Since p is prime, the highest common factor of m and p is 1. Hence, by Theorem B38, the order of m is $p/1 = p$. ■

Here is another enlightening corollary of Theorem B38. It tells us which elements of a group $(\mathbb{Z}_n, +_n)$ are generators of $(\mathbb{Z}_n, +_n)$.

Corollary B40 Generators of $(\mathbb{Z}_n, +_n)$

Let $m \in \mathbb{Z}_n$. Then m is a generator of the group $(\mathbb{Z}_n, +_n)$ if and only if m is coprime to n .

Proof If $m = 0$, then m is not a generator of $(\mathbb{Z}_n, +_n)$, and m is not coprime to n , so the statement holds for this value of m .

Now suppose that m is any non-zero integer in \mathbb{Z}_n , and let d be the highest common factor of m and n . By Theorem B38, m is a generator of $(\mathbb{Z}_n, +_n)$ if and only if

$$\frac{n}{d} = n,$$

that is,

$$d = 1.$$

This equation holds if and only if m and n are coprime. This completes the proof. ■

You saw an instance of Corollary B40 in Exercise B63, where it was found that the generators of $(\mathbb{Z}_8, +_8)$ are 1, 3, 5 and 7; these are the elements of \mathbb{Z}_8 that are coprime to 8. As another example, notice that it follows from the solution to Exercise B68 that all the non-zero elements of \mathbb{Z}_5 generate $(\mathbb{Z}_5, +_5)$; all the non-zero elements of \mathbb{Z}_5 are coprime to 5, since 5 is prime.

Notice that Corollary B40 tells us that the generators of the group $(\mathbb{Z}_n, +_n)$ are the elements of the set U_n .

Exercise B70

For each of the following groups, write down all the generators of the group.

- (a) $(\mathbb{Z}_7, +_7)$ (b) $(\mathbb{Z}_{10}, +_{10})$

Subgroups of $(\mathbb{Z}_n, +_n)$

We can use Theorem B38 to prove a theorem that describes exactly what the subgroups of $(\mathbb{Z}_n, +_n)$ are, for any integer $n \geq 2$. Before you see this theorem, let us look at two examples of groups $(\mathbb{Z}_n, +_n)$, namely $(\mathbb{Z}_6, +_6)$ and $(\mathbb{Z}_8, +_8)$, and find their subgroups.

By the solution to Worked Exercise B26, the distinct cyclic subgroups of the group $(\mathbb{Z}_6, +_6)$ are

$$\begin{aligned}\langle 0 \rangle &= \{0\}, & \text{of order 1,} \\ \langle 3 \rangle &= \{0, 3\}, & \text{of order 2,} \\ \langle 2 \rangle &= \{0, 2, 4\}, & \text{of order 3,} \\ \langle 1 \rangle &= \mathbb{Z}_6, & \text{of order 6.}\end{aligned}$$

There are no other cyclic subgroups of $(\mathbb{Z}_6, +_6)$, because the subgroup generated by each other element of \mathbb{Z}_6 is the same as one of the subgroups above. For example,

$$\langle 4 \rangle = \{0, 4, 2\} = \{0, 2, 4\} = \langle 2 \rangle.$$

Also, as you saw in Worked Exercise B27, the list above contains *all* the subgroups of $(\mathbb{Z}_6, +_6)$, because $(\mathbb{Z}_6, +_6)$ is cyclic and so all its subgroups are cyclic, by Theorem B36.

The list shows that $(\mathbb{Z}_6, +_6)$ has exactly one cyclic subgroup of order q for each positive factor q of 6, and no other subgroups.

Similarly, by the solution to Exercise B62(b), the complete list of subgroups of the group $(\mathbb{Z}_8, +_8)$ is as follows:

$$\begin{aligned}\langle 0 \rangle &= \{0\}, & \text{of order 1,} \\ \langle 4 \rangle &= \{0, 4\}, & \text{of order 2,} \\ \langle 2 \rangle &= \{0, 2, 4, 6\}, & \text{of order 4,} \\ \langle 1 \rangle &= \mathbb{Z}_8, & \text{of order 8.}\end{aligned}$$

This list shows that $(\mathbb{Z}_8, +_8)$ has exactly one cyclic subgroup of order q for each positive factor q of 8, and no other subgroups.

In general, the following result holds.

Theorem B41 Subgroups of $(\mathbb{Z}_n, +_n)$

The group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order q for each positive factor q of n , and no other subgroups.

- The subgroup of order 1 is generated by 0.
- For each other factor q of n , the subgroup of order q is generated by d , where $qd = n$.

Proof Since $(\mathbb{Z}_n, +_n)$ is a cyclic group, all its subgroups are cyclic, by Theorem B36.

There is a cyclic subgroup of order 1, namely the subgroup generated by 0. Now let q be any factor of n other than 1, and let d be given by $qd = n$. Then d is a factor of n , so the highest common factor of d and n is d , and hence, by Theorem B38, d generates a cyclic subgroup of order $n/d = q$.

So we have described one cyclic subgroup of order q for each positive factor q of n .

We now show that there are no further cyclic subgroups of $(\mathbb{Z}_n, +_n)$. Let m be any non-zero integer in \mathbb{Z}_n , and consider the cyclic subgroup $\langle m \rangle$. Let d be the highest common factor of m and n . Then m is a multiple of d , so $m \in \langle d \rangle$ and hence $\langle m \rangle$ is a subgroup of $\langle d \rangle$, by Theorem B32. But, by Theorem B38, the subgroups $\langle m \rangle$ and $\langle d \rangle$ have the same order, namely n/d , so they must be equal. Hence the subgroup $\langle m \rangle$ is the same as one of the subgroups already described. So there are no further cyclic subgroups. ■

Exercise B71

Using Theorem B41, find all the subgroups of each of the following groups. Give a list in which each subgroup appears exactly once.

- (a) $(\mathbb{Z}_{12}, +_{12})$ (b) $(\mathbb{Z}_9, +_9)$ (c) $(\mathbb{Z}_{11}, +_{11})$

Unfortunately, finding all the subgroups of a group is usually a far more difficult task than it is for one of the groups $(\mathbb{Z}_n, +_n)$.

Connections between cyclic groups

To conclude our discussion of cyclic groups, let us compare two particular cyclic groups of order 4.

The group $(S^+(\square), \circ)$ of direct (that is, rotational) symmetries of the square is a cyclic group of order 4. It is generated by a , the rotation through $\pi/2$, as shown in Figure 26. (The non-identity elements of $S^+(\square)$ are illustrated in Figure 27.)

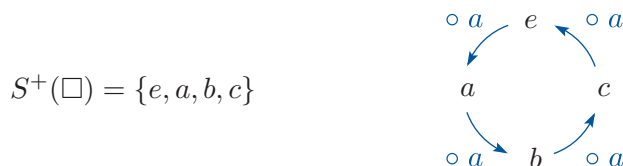


Figure 26 The cyclic group $(S^+(\square), \circ)$

The group $(\mathbb{Z}_4, +_4)$ is a cyclic group of order 4 that is generated by the element 1, as shown in Figure 28.



Figure 28 The cyclic group $(\mathbb{Z}_4, +_4)$

The diagrams in Figures 26 and 28 are very similar. If we take the diagram in Figure 26 and replace the elements e , a , b and c by 0, 1, 2 and 3 using the ‘matching’

$$\begin{array}{cccc} e & a & b & c \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & 3 \end{array},$$

and also replace the operation \circ by the operation $+_4$, then we obtain the diagram in Figure 28. So, *structurally*, these two groups are identical: it is just the names of the elements and the names of the binary operations that differ. Just as the element a generates the first group $(S^+(\square), \circ)$, so the corresponding element, 1, generates the second group $(\mathbb{Z}_4, +_4)$; and just as the element b in $(S^+(\square), \circ)$ has order 2, so its corresponding element, 2, in $(\mathbb{Z}_4, +_4)$ has order 2. Similarly, just as e is the identity element of the first group, so its corresponding element, 0, is the identity element of the second group. Any other cyclic group of order 4 has exactly the same structure as these two groups.

In the same way, for any positive integer n , all the cyclic groups of order n have exactly the same structure as each other.

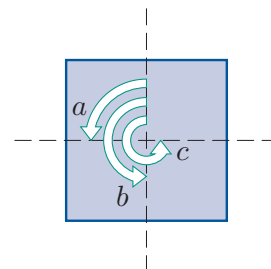


Figure 27 $S^+(\square)$

Proof of Theorem B38 (optional)

Finally in this subsection, here is a proof of Theorem B38, as promised. It will not be assessed: read it if you are interested and have plenty of time – skip it otherwise. The theorem is as follows.

Theorem B38

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. Then m has order n/d , where d is the highest common factor of m and n .

We start with a lemma that is a particular case of Theorem B38, namely the case where m is a factor of n . This case is much easier to prove.

Lemma B42

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. If m is a factor of n , then m has order n/m .

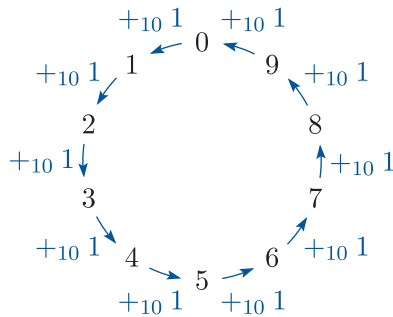


Figure 29 The cycle of multiples of 1 in $(\mathbb{Z}_{10}, +_{10})$

To see why this lemma holds, consider, for example, the integer 2 in $(\mathbb{Z}_{10}, +_{10})$. Repeatedly adding 2 in \mathbb{Z}_{10} is the same as moving 2 places at a time round the cycle in Figure 29. If we start from 0 and add 2 a total of $10/2 = 5$ times then we get back to 0, whereas if we add 2 any fewer than 5 times then we do not get back to 0. So the order of 2 in $(\mathbb{Z}_{10}, +_{10})$ is 5.

Generalising this argument gives the following proof of Lemma B42.

Proof of Lemma B42 Suppose that m is a factor of n . Repeatedly adding m in $(\mathbb{Z}_n, +_n)$ is the same as moving m places at a time round the cycle in Figure 30. If we start from 0 and add m a total of n/m times then we get back to 0, whereas if we add m any fewer than n/m times then we do not get back to 0. Hence the order of m in $(\mathbb{Z}_n, +_n)$ is n/m . ■

Now here is the proof of Theorem B38. You will see that in this proof we use both the result of Lemma B42, and the ideas used in the proof of Lemma B42.

Proof of Theorem B38 Let m be a non-zero integer in \mathbb{Z}_n , and let d be the highest common factor of m and n . Then m/d and n/d are coprime integers. Also, since d is a factor of n , the order of d is n/d , by Lemma B42.

We have to show that the order of m is also n/d . First we show that the order of m is *at most* n/d . Consider the cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$, shown in Figure 30.

Suppose that we start from 0 and move round m places at a time, a total of n/d times. This is the same as starting from 0 and moving round a total of mn/d places. Since m/d is an integer, the number mn/d is a multiple of n , so we end up at 0. Hence the order of m is indeed at most n/d .

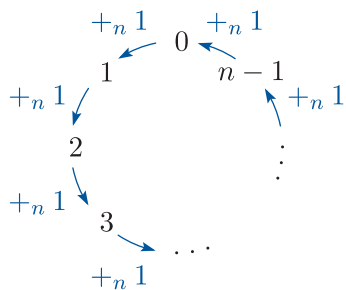


Figure 30 The cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$

Now we show that the order of m cannot be less than n/d . We use a contradiction argument. Suppose that the order of m is r , where $1 \leq r < n/d$. Then if we start from 0 in the cycle in Figure 30 and move round m places at a time, a total of r times, we end up at 0. Hence

$$rm = kn \quad (4)$$

for some natural number k . Dividing both sides of this equation by d and rearranging slightly, we obtain

$$r \frac{m}{d} = k \frac{n}{d}.$$

Now remember that m/d and n/d are coprime integers. The equation above tells us that m/d is a factor of $k(n/d)$, and hence, since m/d is coprime to n/d , it follows that m/d is a factor of k . Therefore the number $k/(m/d)$, that is, kd/m , is an integer.

If we now go back to equation (4), multiply it through by d and divide it through by m , then we obtain

$$rd = \frac{kd}{m}n.$$

Thus rd is an integer multiple of n . So if we start from 0 in the cycle in Figure 30 and move round d places at a time, a total of r times, then we end up at 0. But $1 \leq r < n/d$, so this contradicts the fact that the order of d is n/d . Thus the order of m cannot be less than n/d .

This completes the proof that the order of m is n/d . ■

4 Isomorphisms

Near the end of the previous section, just before the proof of Theorem B38, it was pointed out that the cyclic groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ of order 4 are structurally identical, and that in fact all the cyclic groups of any particular order are structurally identical to each other. In this section we will explore the idea of structurally identical groups for groups in general, both cyclic and non-cyclic.

4.1 Cayley tables of groups of orders 4 and 6

One way to compare the structures of two finite groups is to look at their Cayley tables. In this subsection we will do this for some groups of orders 4 and 6.

Cayley tables of groups of order 4

Let us start by looking at the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ again, this time comparing their structures by looking at their Cayley tables, which are as follows.

\circ	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$(S^+(\square), \circ)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_4, +_4)$

You can see that if we take the Cayley table of $(S^+(\square), \circ)$, and replace the elements e, a, b and c by 0, 1, 2 and 3 using the same matching as before, namely

e	a	b	c
\updownarrow	\updownarrow	\updownarrow	\updownarrow
0	1	2	3

,

and also replace the operation \circ by the operation $+_4$, then we obtain the Cayley table of $(\mathbb{Z}_4, +_4)$. This shows that the two groups are structurally identical, as we also found in Subsection 3.4.

The Cayley table of $(\mathbb{Z}_4, +_4)$ can be obtained from the Cayley table of $(S^+(\square), \circ)$ by ‘renaming’ the elements because the two Cayley tables have exactly the same pattern. They both have the pattern of bottom left to top right diagonal stripes shown in Figure 31.



Figure 31 The pattern of the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$

Now let us look at another group of order 4, and try to determine whether it has the same structure as $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$. The group $(\mathbb{Z}_5^*, \times_5)$ has the following Cayley table.

\times_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}_5^*, \times_5)$

The pattern in this Cayley table, shown in Figure 32, is different from the pattern in the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$.



Figure 32 The pattern of the Cayley table of $(\mathbb{Z}_5^*, \times_5)$

However, it is possible to rearrange the Cayley table of $(\mathbb{Z}_5^*, \times_5)$ to make it have the same pattern as the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$, that is, the pattern of diagonal stripes in Figure 31. One way to do this is to interchange the positions of the elements 3 and 4 in the borders of the table (this must be done in both borders) and rearrange the entries in the body of the table accordingly.

To rearrange the entries in the body of the table, we can either just fill them in again using the rearranged table borders, or we can take the original table, interchange the last two columns to obtain an intermediate table, and then interchange the last two rows of this intermediate table to obtain the new table, as shown below.

\times_5	1	2	3	4		\times_5	1	2	4	3		\times_5	1	2	4	3
1	1	2	3	4		1	1	2	4	3		1	1	2	4	3
2	2	4	1	3	\rightarrow	2	2	4	3	1	\rightarrow	2	2	4	3	1
3	3	1	4	2	swap	3	3	1	2	4	swap	4	4	3	1	2
4	4	3	2	1	columns	4	4	3	1	2	rows	3	3	1	2	4
					3,4						3,4					
	original						intermediate						rearranged			
	table						table						table			

Either way, we end up with the rearranged Cayley table of $(\mathbb{Z}_5^*, \times_5)$ shown on the right above. This table has the same pattern of diagonal stripes as the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$. Hence the group $(\mathbb{Z}_5^*, \times_5)$ is structurally identical to the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$.

Exercise B72

For each of the following pairs of groups, write down a matching between the elements of the first group and the elements of the second group, such that if the elements in the Cayley table of the first group are replaced according to this matching, then the Cayley table of the second group is obtained.

- (a) $(S^+(\square), \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ (b) $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \times_5)$

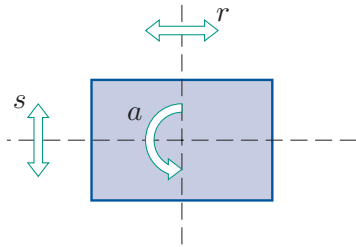


Figure 33 $S(\square)$

It is important to remember that when you rearrange the entries in the borders of a Cayley table, you must rearrange both borders in the same way. In a Cayley table the entries in the two borders must be in the same order.

The three groups of order 4 that we have looked at so far in this subsection all have Cayley tables that can be rearranged into the pattern of diagonal stripes shown in Figure 31. Let us now look at two more groups of order 4, and try to determine whether their Cayley tables can also be rearranged into this pattern. We will look at the symmetry group of the rectangle, $(S(\square), \circ)$, and the group (U_8, \times_8) . The non-identity elements of $S(\square)$ are shown in Figure 33. Remember that U_8 is the set of integers in \mathbb{Z}_8 that are coprime to 8, that is, $U_8 = \{1, 3, 5, 7\}$. The Cayley tables of these two groups are as follows.

\circ	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\square), \circ)$

\times_8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

(U_8, \times_8)

These two Cayley tables do not currently have the pattern of diagonal stripes. They do, however, have the same pattern as each other, shown in Figure 34, so the groups $(S(\square), \circ)$ and (U_8, \times_8) are structurally identical to each other.



Figure 34 The pattern of the Cayley tables of $(S(\square), \circ)$ and (U_8, \times_8)



Figure 35 The pattern (diagonal stripes) of the Cayley tables of $(S^+(\square), \circ)$, $(\mathbb{Z}_4, +_4)$ and \mathbb{Z}_5^*

To determine whether these two groups are also structurally identical to the first three groups that we looked at in this subsection, we need to find out whether their Cayley tables can be rearranged into the pattern of diagonal stripes in Figure 31, which is repeated in Figure 35. Now, notice that in the pattern of diagonal stripes, the main diagonal (the diagonal from top left to bottom right) contains two different elements, each appearing twice. However, in the groups $(S(\square), \circ)$ and (U_8, \times_8) , all the elements are self-inverse, so no matter how we rearrange the borders of their Cayley tables, the four cells on the main diagonal will contain four occurrences of the identity element. So the Cayley tables of $(S(\square), \circ)$ and (U_8, \times_8) cannot be rearranged into the pattern of diagonal stripes in Figure 35.

Thus we have found two different structures for groups of order 4, given by the patterns shown in Figure 36.



Figure 36 The patterns of the Cayley tables of $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$, respectively

It turns out that, for *any* group of order 4, its Cayley table can be rearranged (if necessary) to make it have one of the two patterns in Figure 36. So every group of order 4 has the same structure as one of the groups $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$. You will see a proof of this fact in Unit B4 *Lagrange's Theorem and small groups*.

Notice that both of the patterns in Figure 36 are symmetric with respect to the main diagonal, so every group of order 4 is abelian.

Exercise B73

For each of the following groups of order 4, write down its Cayley table and determine whether it has the same structure as $(\mathbb{Z}_4, +_4)$ or $(S(\square), \circ)$.

- (a) (U_{12}, \times_{12}) (b) (U_{10}, \times_{10})

Cayley tables for groups of order 6

We now look briefly at groups of order 6. Consider the groups $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$, both of which have order 6. The non-identity elements of $S(\triangle)$ are shown in Figure 37. The Cayley tables of the two groups are as follows.

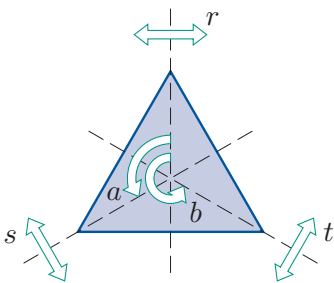


Figure 37 $S(\triangle)$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\mathbb{Z}_6, +_6)$

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$(S(\triangle), \circ)$

These Cayley tables have the patterns shown in Figure 38.

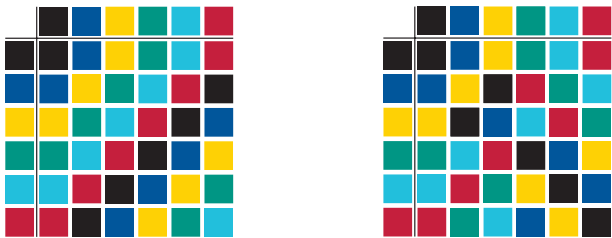


Figure 38 The patterns of the Cayley tables of $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$, respectively

Notice that in the pattern of the Cayley table of $(\mathbb{Z}_6, +_6)$, the main diagonal contains three different elements, each appearing twice. However, the group $(S(\triangle), \circ)$ has four self-inverse elements, so no matter how we arrange the borders of its Cayley table, the main diagonal will contain four occurrences of the identity element e . Hence it is not possible to rearrange the Cayley table of $(S(\triangle), \circ)$ into the pattern of the Cayley table of $(\mathbb{Z}_6, +_6)$, and therefore these two groups have different structures.

Thus we have found two different structures for groups of order 6, as given by the patterns shown in Figure 38. It turns out that for any group of order 6, its Cayley table can be rearranged (if necessary) to make it have one of the two patterns in Figure 38. In other words, every group of order 6 has the same structure as one of the groups $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$. You will see a proof of this fact in Unit B4.

Notice that the pattern on the left in Figure 38 is symmetric with respect to the main diagonal, so a group with this pattern is an abelian group. In contrast, a group with the pattern on the right is non-abelian.

Notice also that the Cayley table of $(\mathbb{Z}_6, +_6)$ has a pattern of diagonal stripes similar to that of the Cayley table of $(\mathbb{Z}_4, +_4)$. In general, for any integer $n \geq 2$, the Cayley table of $(\mathbb{Z}_n, +_n)$ has a pattern of bottom left to top right diagonal stripes when the elements in the borders are listed in the natural order.

4.2 Isomorphic groups

In this subsection we will formalise exactly what it means for two groups to be ‘structurally identical’ to each other. We will initially consider finite groups, as we did in the last subsection.

You have seen that two finite groups have the same structure if there is a ‘matching’ between the elements of the two groups such that when we replace all the elements in a Cayley table for one group using this matching, then we obtain a Cayley table for the other group.

For example, the two groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ have the same structure because, as you should have found in Exercise B72(a), if we take a Cayley table of $(S^+(\square), \circ)$ and replace the elements e, a, b and c of $S^+(\square)$ by the elements 1, 2, 3 and 4 of \mathbb{Z}_5^* using the matching

$$\begin{array}{cccc} e & a & b & c \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 4 & 3 \end{array},$$

then we obtain a Cayley table for $(\mathbb{Z}_5^*, \times_5)$:

$$\begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array} \longrightarrow \begin{array}{c|cccc} \times_5 & 1 & 2 & 4 & 3 \\ \hline 1 & 1 & 2 & 4 & 3 \\ 2 & 2 & 4 & 3 & 1 \\ 4 & 4 & 3 & 1 & 2 \\ 3 & 3 & 1 & 2 & 4 \end{array}$$

$(S^+(\square), \circ) \qquad (\mathbb{Z}_5^*, \times_5)$

It does not matter here that the elements in the borders of the Cayley table for $(\mathbb{Z}_5^*, \times_5)$ are not listed in the usual order: all that matters is that the table is a correct Cayley table for $(\mathbb{Z}_5^*, \times_5)$.

It is helpful to think of a matching between the elements of two groups as a mapping, say ϕ , from the first group to the second. For example, for the two groups above we have the mapping

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 1 \\ a &\longmapsto 2 \\ b &\longmapsto 4 \\ c &\longmapsto 3. \end{aligned}$$

If a mapping ϕ from one group to another is to transform a Cayley table for the first group into a Cayley table for the second group, then it must match up *all* the elements of the two groups *one-to-one*. In other words, it must be a one-to-one and onto mapping (that is, a *one-to-one correspondence*). It must also have a further property.

To understand why a further property is necessary, suppose that we replace the elements in the Cayley table for the group $(S^+(\square), \circ)$ by the elements of the group $(\mathbb{Z}_5^*, \times_5)$ using the following one-to-one and onto mapping:

$$\begin{aligned}\phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 2 \\ a &\longmapsto 3 \\ b &\longmapsto 4 \\ c &\longmapsto 1.\end{aligned}$$

This has the following effect:

$$\begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array} \longrightarrow \begin{array}{c|cccc} & 2 & 3 & 4 & 1 \\ \hline 2 & 2 & 3 & 4 & 1 \\ 3 & 3 & 4 & 1 & 2 \\ 4 & 4 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 4 \end{array}$$

$(S^+(\square), \circ)$

You can see that although we have obtained a table whose entries are the elements of the group $(\mathbb{Z}_5^*, \times_5)$, *it is not a correct Cayley table for $(\mathbb{Z}_5^*, \times_5)$* . For example, $2 \times_5 2 = 4$, but the cell in the table that should contain the composite $2 \times_5 2$ actually contains the element 2.

So if a mapping ϕ from one group to another is to have the effect of transforming a Cayley table for one group into a Cayley table for another group, then not only must it be one-to-one and onto, but it must also have a further property that ensures that the resulting Cayley table is correct.

To see what this property must be, consider two abstract finite groups, (G, \circ) and $(H, *)$, say. Suppose that we take a Cayley table for (G, \circ) and replace all the elements using a one-to-one and onto mapping $\phi : G \longrightarrow H$. Consider any two elements x and y of G , and their composite $x \circ y$ in the Cayley table for (G, \circ) , as illustrated on the left below. In the transformed table, these three elements are replaced by $\phi(x)$, $\phi(y)$ and $\phi(x \circ y)$, as illustrated on the right.

$$\begin{array}{c|cccc} \circ & \cdots & y & \cdots \\ \hline \vdots & & \vdots & \\ x & \cdots & x \circ y & \cdots \\ \vdots & & \vdots & \end{array} \longrightarrow \begin{array}{c|cccc} * & \cdots & \phi(y) & \cdots \\ \hline \vdots & & \vdots & \\ \phi(x) & \cdots & \phi(x \circ y) & \cdots \\ \vdots & & \vdots & \end{array}$$

(G, \circ) $(H, *)$

If the table obtained is to be a correct Cayley table for $(H, *)$, then the entry in the cell with row label $\phi(x)$ and column label $\phi(y)$ must be equal to $\phi(x) * \phi(y)$, so we must have

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

This applies to *any* elements x and y of G , so the property that we need the mapping ϕ to have is

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G. \quad (5)$$

So saying that two finite groups (G, \circ) and $(H, *)$ have the same structure is the same as saying that there exists a one-to-one and onto mapping ϕ with property (5).

This also applies to *infinite* groups; the only difference is that we cannot write down Cayley tables for such groups.

The term that we use in group theory to describe groups as ‘structurally identical’ is *isomorphic*. So we make the following definition.

Definition

Two groups (G, \circ) and $(H, *)$ are **isomorphic** if there exists a mapping $\phi : G \rightarrow H$ with the following properties.

(a) ϕ is one-to-one and onto.

(b) For all $x, y \in G$,

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

Such a mapping ϕ is called an **isomorphism**.

We use the symbol \cong to denote the relation ‘is isomorphic to’.

That is, we write

$$(G, \circ) \cong (H, *)$$

to assert that the groups (G, \circ) and $(H, *)$ are isomorphic.

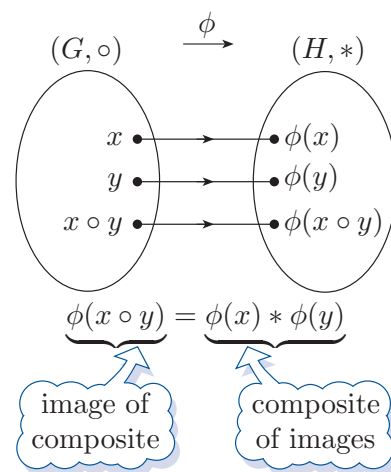


Figure 39 An isomorphism ϕ

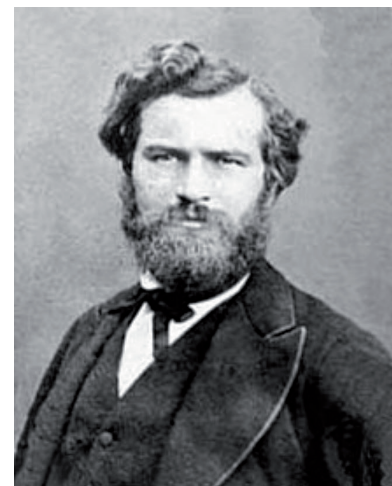
This definition is illustrated in Figure 39.

You have seen that we sometimes write a group (G, \circ) simply as G , when the group operation is understood from the context. Accordingly, we sometimes write $(G, \circ) \cong (H, *)$ simply as $G \cong H$.

Also, we often write an isomorphism $\phi : G \rightarrow H$ as $\phi : (G, \circ) \rightarrow (H, *)$, to indicate the binary operations of the two groups G and H .

Remember that, informally, two groups are isomorphic if they have exactly the same structure, even though their elements and binary operation may be different. An isomorphism maps each element of one group to an element ‘that has the same role’ in the structure of the other group.

The term *isomorphism* was introduced into group theory by the French mathematician Camille Jordan (1838–1922) in his classic treatise *Traité des substitutions et des équations algébriques* (*Treatise on Substitutions and Algebraic Equations*) of 1870, the book in which many modern notions of group theory first appear. The term was used earlier in crystallography.



Camille Jordan

Here is a simple property of isomorphic groups.

Theorem B43

If two groups (G, \circ) and $(H, *)$ are isomorphic, then either (G, \circ) and $(H, *)$ are both finite, with the same order, or (G, \circ) and $(H, *)$ are both infinite.

Proof This follows from the fact that if G and H are isomorphic, then the elements of G can be matched one-to-one with the elements of H . ■

Thus, for example, a group of order 4 cannot be isomorphic to a group of order 6, and a finite group cannot be isomorphic to an infinite group.

The next theorem states some important basic properties of isomorphic groups. These properties are stated in terms of ideas that you met in Unit A3 *Mathematical language*, namely an *equivalence relation* and its constituent properties *reflexivity*, *symmetry* and *transitivity*.

Theorem B44

The relation ‘is isomorphic to’ is an equivalence relation on the collection of all groups. That is, the following three properties hold.

Reflexivity Every group is isomorphic to itself.

Symmetry For any groups (G, \circ) and $(H, *)$, if (G, \circ) is isomorphic to $(H, *)$, then $(H, *)$ is isomorphic to (G, \circ) .

Transitivity For any groups (G, \circ) , $(H, *)$ and (K, \triangle) , if (G, \circ) is isomorphic to $(H, *)$ and $(H, *)$ is isomorphic to (K, \triangle) , then (G, \circ) is isomorphic to (K, \triangle) .

You can see that the properties in the theorem hold, because to say that two groups are isomorphic means that they have the same structure; if you replace the words ‘is isomorphic to’ by the words ‘has the same structure as’, then the properties become almost obvious. The properties can be proved formally using the definition of isomorphic groups given above, but the proofs are not included here.

Since isomorphism is an equivalence relation, the collection of all groups can be partitioned into equivalence classes, which we call **isomorphism classes**, such that two groups belong to the same isomorphism class if they are isomorphic, but belong to different classes otherwise. For example, the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ have the same structure and therefore belong to the same isomorphism class, whereas the groups $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$ have structures different from each other and therefore belong to different isomorphism classes.

All the groups in any particular isomorphism class have the same order, since groups of different orders are not isomorphic. You saw earlier that there are only two possible structures for groups of order 4, so there are only two isomorphism classes containing groups of order 4. These are as follows.

- The class of cyclic groups of order 4. Its members include the three groups $(S^+(\square), \circ)$, $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \times_5)$. Each group in this class has exactly two self-inverse elements.
- The class whose members include $(S(\square), \circ)$ and (U_8, \times_8) . In each group in this class all four elements are self-inverse.

We use the symbol C_4 to denote a standard, abstract group with the structure of the groups in the first class above, and we refer to it as *the cyclic group of order 4*. We use the symbol V to denote a standard, abstract group with the structure of the groups in the second class above, and we refer to this group as the **Klein four-group**.

The Klein four-group is named after the German mathematician Felix Klein (1849–1925). The symbol V used for the Klein four-group stands for *Viergruppe*, which was the name given to it by Klein in 1884 in his *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade* (*Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*). It was named for Klein by the Dutch mathematician Bartel van der Waerden (1903–1996) in his *Moderne Algebra* (1930), his influential textbook on abstract algebra. Van der Waerden had studied at the University of Göttingen where Klein had established one of the world's leading mathematics research centres.

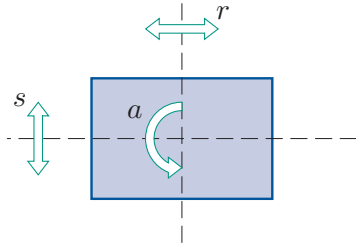


Felix Klein

You have seen that there are only two possible structures for groups of order 6, so there are also only two isomorphism classes containing groups of order 6. These are the class containing $(\mathbb{Z}_6, +_6)$ and the class containing $(S(\triangle), \circ)$. We use the symbol C_6 to denote a standard, abstract group with the structure of the groups in the first of these two classes, and we refer to it as *the cyclic group of order 6*. You will learn more about the structure of groups in the second class in Units B3 and B4.

One way to show that two *finite* groups are isomorphic is to rearrange their Cayley tables to have the same pattern, as you saw in the last subsection. Once you have done that, you can obtain an isomorphism from one of the groups to the other by matching up corresponding elements in the rearranged Cayley tables.

For example, at the start of this subsection you saw Cayley tables of the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ rearranged to have the same pattern, and a one-to-one correspondence $\phi : S^+(\square) \rightarrow \mathbb{Z}_5^*$ that matches up corresponding elements in the rearranged Cayley tables. This mapping ϕ is an isomorphism.

Figure 40 $S(\square)$

Exercise B74

In Exercise B73, near the end of the previous subsection, you should have found the following (though the word ‘isomorphic’ was not used there).

- (a) $(S(\square), \circ)$ is isomorphic to (U_{12}, \times_{12}) .
- (b) $(\mathbb{Z}_4, +_4)$ is isomorphic to (U_{10}, \times_{10}) .

In each case, by using the solution to Exercise B73, write down an isomorphism from the first group to the second group. (The non-identity elements of $(S(\square), \circ)$ are illustrated in Figure 40 for convenience.)

To show that two *infinite* groups are isomorphic you have to show algebraically that there is an isomorphism from one of the groups to the other, as illustrated in the next worked exercise.

Worked Exercise B29

Let (G, \times) be the cyclic subgroup of the group (\mathbb{R}, \times) generated by the element 2; the set G is given by

$$G = \{2^k : k \in \mathbb{Z}\}.$$

Prove that (G, \times) is isomorphic to the group $(\mathbb{Z}, +)$ by showing that the following mapping ϕ is an isomorphism:

$$\begin{aligned}\phi: G &\longrightarrow \mathbb{Z} \\ 2^k &\longmapsto k.\end{aligned}$$

Solution

By the definition of an isomorphism, we must show that ϕ is one-to-one and onto, and that for all $2^j, 2^k \in G$,

$$\phi(2^j \times 2^k) = \phi(2^j) + \phi(2^k).$$

(The binary operations on the left and right in this equation are those of (G, \times) and $(\mathbb{Z}, +)$, respectively.)

First we check that ϕ is one-to-one. Let $2^j, 2^k \in G$ and suppose that $\phi(2^j) = \phi(2^k)$; that is,

$$j = k.$$

It follows that $2^j = 2^k$. Thus ϕ is one-to-one.

Also, ϕ is onto because each element $k \in \mathbb{Z}$ is the image under ϕ of the element $2^k \in G$.

Finally, for all $2^j, 2^k \in G$,

$$\phi(2^j \times 2^k) = \phi(2^{j+k}) = j + k = \phi(2^j) + \phi(2^k).$$

Thus ϕ is an isomorphism, so $(G, \times) \cong (\mathbb{Z}, +)$.

Notice that in Worked Exercise B29 we took our two arbitrary elements of (G, \times) to be 2^j and 2^k , where $j, k \in \mathbb{Z}$. We could alternatively have taken our two arbitrary elements to be x and y , and then gone on to state that it follows that $x = 2^j$ and $y = 2^k$, where $j, k \in \mathbb{Z}$. However, it is slightly more efficient to take our two elements of (G, \times) to be 2^j and 2^k in the first place. This type of shortcut is sometimes convenient in algebraic arguments, but it is fine to use either approach.

Exercise B75

Prove that the group $(\mathbb{Z}, +)$ is isomorphic to the group $(6\mathbb{Z}, +)$ by showing that the following mapping ϕ is an isomorphism:

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow 6\mathbb{Z} \\ n &\longmapsto 6n.\end{aligned}$$

Once we have built up some knowledge about isomorphism classes of groups, we may be able to use it to help us show that two groups, finite or infinite, are isomorphic. In the next worked exercise this method is used to show that two groups of order 4 are isomorphic.

Worked Exercise B30

Show that the groups $(\{1, -1, i, -i\}, \times)$ (where $i^2 = -1$) and $(\mathbb{Z}_4, +_4)$ are isomorphic.

(You saw that $(\{1, -1, i, -i\}, \times)$ is a group in Exercise B37.)

Solution

Every group of order 4 is isomorphic to either the cyclic group C_4 , which has exactly two self-inverse elements, or to the Klein four-group V , which has four self-inverse elements.

In the group $(\{1, -1, i, -i\}, \times)$, which has identity 1, we have

$$1 \times 1 = 1, \quad (-1) \times (-1) = 1, \quad i \times i = -1, \quad (-i) \times (-i) = -1.$$

So exactly two elements are self-inverse and hence this group is isomorphic to C_4 .

In the group $(\mathbb{Z}_4, +_4)$, which has identity 0, we have

$$0 +_4 0 = 0, \quad 1 +_4 1 = 2, \quad 2 +_4 2 = 0, \quad 3 +_4 3 = 2.$$

So again exactly two elements are self-inverse and hence this group is isomorphic to C_4 .

Since both groups are isomorphic to C_4 , they are isomorphic to each other.

Exercise B76

Show that the groups (U_{12}, \times_{12}) and $(S(\square), \circ)$ are isomorphic, without using Cayley tables.

The strategy below summarises some methods that you can use for showing that two groups are isomorphic.

Strategy B4

To show that two groups are isomorphic, try one of the following methods.

- Use facts that you know about the structures of the groups (such as whether they are cyclic, or abelian, and how many self-inverse elements they have), together with facts that you know about isomorphism classes.
- If the groups have small finite order, rearrange their Cayley tables to have the same pattern.
- If the groups are infinite or have large finite order, show algebraically that there is an isomorphism from one group to the other.

To help you identify a suitable rearrangement of a Cayley table, or an isomorphism, try using the properties in Theorems B45 and B46 in the next subsection.

Finally in this subsection, here is a comment that you might find interesting, though it is quite complicated and you can skip it if you wish. Isomorphisms provide an explanation of how some groups with unusual binary operations arise. For example, Worked Exercise B18 in Subsection 1.2 involved a group $(X, *)$, where

$$X = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}$$

and $*$ is the binary operation on X defined by

$$(a, b) * (c, d) = (ac, ad + b).$$

This seemingly strange binary operation is revealed as something much more natural if we consider a particular group isomorphic to the group $(X, *)$. It is straightforward to show that the set, A say, of all real functions of the form

$$x \mapsto ax + b \quad (a, b \in \mathbb{R}, a \neq 0)$$

forms a group under function composition (it is known as the *one-dimensional affine group over the real numbers*), and that the mapping ϕ from (A, \circ) to $(X, *)$ given by

$$\text{the function } x \mapsto ax + b \text{ maps to the point } (a, b)$$

is an isomorphism. If we let $f(x) = ax + b$ and $g(x) = cx + d$ be two functions in A , then their composite $f \circ g$ is given by

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) \\ &= f(cx + d) \\ &= a(cx + d) + b \\ &= acx + ad + b, \end{aligned}$$

which demonstrates how the unusual binary operation $*$ of the group $(X, *)$ arises. The point $(ac, ad + b)$ is the image of the function $f \circ g$ above under the isomorphism ϕ .

4.3 Properties of isomorphisms

In this subsection you will meet four theorems that describe some useful properties of isomorphisms and isomorphic groups. These are properties that you would expect to hold simply because isomorphic groups are groups with the same structure, and isomorphisms match up elements that ‘have the same role’ in that structure. However, formal proofs, using the definition of an isomorphism, are also provided.

Here is the first of these four theorems.

Theorem B45

Let (G, \circ) and $(H, *)$ be groups with identities e_G and e_H , respectively. Any isomorphism $\phi : (G, \circ) \rightarrow (H, *)$ has the following properties.

(a) ϕ matches the identity elements:

$$\phi(e_G) = e_H.$$

(b) ϕ matches inverses: for each $g \in G$,

$$\phi(g^{-1}) = (\phi(g))^{-1}.$$

(c) ϕ matches powers of each element: for each $g \in G$ and each $k \in \mathbb{Z}$,

$$\phi(g^k) = (\phi(g))^k.$$

The properties of isomorphisms in Theorem B45 are illustrated in Figure 41.

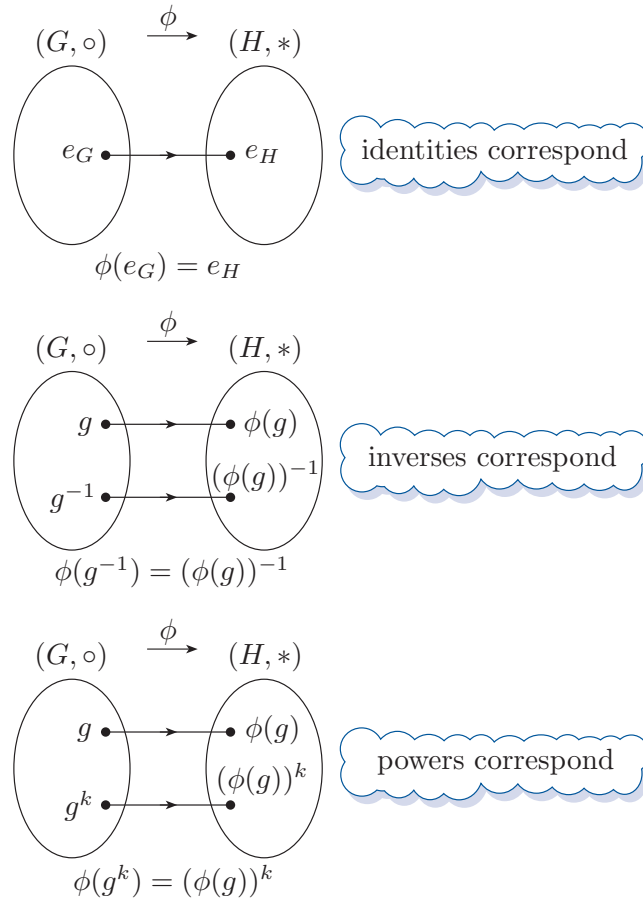


Figure 41 Basic properties of isomorphisms

Proof of Theorem B45

Let $\phi: (G, \circ) \rightarrow (H, *)$ be an isomorphism.

(a) We have

$$e_G \circ e_G = e_G.$$

Applying the isomorphism ϕ gives

$$\phi(e_G \circ e_G) = \phi(e_G).$$

Since ϕ is an isomorphism, this gives

$$\phi(e_G) * \phi(e_G) = \phi(e_G),$$

and hence

$$\phi(e_G) * \phi(e_G) = \phi(e_G) * e_H.$$

Applying the Left Cancellation Law now gives

$$\phi(e_G) = e_H.$$

(b) Let $g \in G$. Then

$$g \circ g^{-1} = e_G = g^{-1} \circ g.$$

Applying the isomorphism ϕ gives

$$\phi(g \circ g^{-1}) = \phi(e_G) = \phi(g^{-1} \circ g).$$

Since ϕ is an isomorphism and since $\phi(e_G) = e_H$, this gives

$$\phi(g) * \phi(g^{-1}) = e_H = \phi(g^{-1}) * \phi(g).$$

This shows that $\phi(g^{-1})$ is the inverse of $\phi(g)$ in H , that is,

$$\phi(g^{-1}) = (\phi(g))^{-1}.$$

(c) The proof of this property is omitted here as it is quite lengthy, but the next exercise shows that the property is true for $k = 2$, and asks you to deduce that it is true for $k = 3$. Note also that property (b) above is the case $k = -1$. The full proof is included in Book E *Group theory 2*. ■

Exercise B77

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism, and let g be an element of G . Then, since ϕ is an isomorphism,

$$\phi(g \circ g) = \phi(g) * \phi(g),$$

and this equation can be written in terms of powers as

$$\phi(g^2) = (\phi(g))^2, \tag{6}$$

which is Theorem B45(c) in the case $k = 2$.

By writing $g^3 = g^2 \circ g$ and using the fact that ϕ is an isomorphism, together with equation (6), prove that

$$\phi(g^3) = (\phi(g))^3.$$

As usual with results in group theory, Theorem B45 is stated in multiplicative notation, but you need to be able to apply it to additive groups as well as to multiplicative groups. For example, property (c) in the theorem, with $k = 3$, tells you that if (G, \times) and $(H, +)$ are groups and $\phi : (G, \times) \longrightarrow (H, +)$ is an isomorphism, then for any element $g \in G$ we have

$$\phi(g^3) = 3\phi(g)$$

(which we can also write as

$$\phi(g \times g \times g) = \phi(g) + \phi(g) + \phi(g).)$$

The next theorem gives some further useful properties of isomorphisms.

Theorem B46

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism. Let $g \in G$.

- If g has order n , then so does $\phi(g)$.
- If g has infinite order, then so does $\phi(g)$.

Proof Let the identities of (G, \circ) and $(H, *)$ be e_G and e_H , respectively. For any $k \in \mathbb{N}$, the equation

$$g^k = e_G$$

is equivalent to the equation

$$\phi(g^k) = \phi(e_G),$$

(since ϕ is a one-to-one mapping), and this equation is in turn equivalent to the equation

$$(\phi(g))^k = e_H$$

(by properties (a) and (c) in Theorem B45).

Hence the set of integers k for which $g^k = e_G$ is exactly the same as the set of integers k for which $(\phi(g))^k = e_H$. The two statements in the theorem follow immediately. ■

The third theorem in this subsection tells us that, as you would expect, isomorphisms match up subgroups. For example, consider the isomorphic groups $(S^+(\square), \circ)$ and (\mathbb{Z}_5, \times_5) , and the following isomorphism between them, which you met in Subsection 4.2:

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 1 \\ a &\longmapsto 2 \\ b &\longmapsto 4 \\ c &\longmapsto 3, \end{aligned}$$

We know that $K = \{e, b\}$ is a subgroup of $(S^+(\square), \circ)$ (it is the cyclic subgroup generated by b). Correspondingly, the image of this subgroup under ϕ , which is

$$\phi(K) = \{\phi(k) : k \in K\} = \{\phi(e), \phi(b)\} = \{1, 4\},$$

is a subgroup of (\mathbb{Z}_5, \times_5) . Here is the general result.

Theorem B47

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism. If K is a subgroup of (G, \circ) , then

$$\phi(K) = \{\phi(k) : k \in K\}$$

is a subgroup of $(H, *)$.

Proof Certainly $\phi(K)$ is a subset of H . We show that $(\phi(K), *)$ is a subgroup of $(H, *)$ by showing that it satisfies the three subgroup properties.

SG1 Closure

Let $l_1, l_2 \in \phi(K)$; then $l_1 = \phi(k_1)$ and $l_2 = \phi(k_2)$ for some $k_1, k_2 \in K$. Hence

$$\begin{aligned} l_1 * l_2 &= \phi(k_1) * \phi(k_2) \\ &= \phi(k_1 \circ k_2) \quad (\text{since } \phi \text{ is an isomorphism}). \end{aligned}$$

Now $k_1 \circ k_2 \in K$, because K is a subgroup of (G, \circ) , so this shows that $l_1 * l_2 \in \phi(K)$. Thus $\phi(K)$ is closed under $*$.

SG2 Identity

Let e_G and e_H be the identities of (G, \circ) and $(H, *)$, respectively. Then $\phi(e_G) = e_H$, by Theorem B45(a). Now $e_G \in K$, because K is a subgroup of (G, \circ) , so this shows that $e_H \in \phi(K)$.

SG3 Inverses

Let $l \in \phi(K)$; then $l = \phi(k)$ for some $k \in K$. Hence

$$\begin{aligned} l^{-1} &= (\phi(k))^{-1} \\ &= \phi(k^{-1}) \quad (\text{by Theorem B45(b)}). \end{aligned}$$

Now $k^{-1} \in K$, because K is a subgroup of (G, \circ) , so this shows that $l^{-1} \in \phi(K)$. Thus $\phi(K)$ contains the inverse of each of its elements.

Hence $(\phi(K), *)$ satisfies the three subgroup properties, and so is a subgroup of $(H, *)$. ■

The final theorem in this subsection states some properties of isomorphic groups. As with the earlier properties, you would expect these properties to hold, simply because saying that two groups are isomorphic means that they have the same structure. However, formal proofs are provided.

Theorem B48

Let (G, \circ) and $(H, *)$ be isomorphic groups.

- (a) If (G, \circ) is abelian then so is $(H, *)$.
- (b) If (G, \circ) is cyclic then so is $(H, *)$.

Proof Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism.

- (a) Suppose that (G, \circ) is abelian. We have to show that $(H, *)$ is abelian. Let h_1, h_2 be any elements of H . Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. Since (G, \circ) is abelian, we have

$$g_1 \circ g_2 = g_2 \circ g_1.$$

Hence

$$\phi(g_1 \circ g_2) = \phi(g_2 \circ g_1).$$

Since ϕ is an isomorphism, this gives

$$\phi(g_1) * \phi(g_2) = \phi(g_2) * \phi(g_1),$$

that is,

$$h_1 * h_2 = h_2 * h_1.$$

This shows that $(H, *)$ is abelian.

- (b) Suppose that (G, \circ) is cyclic, generated by a . We will show that $(H, *)$ is also cyclic, generated by $\phi(a)$. Let h be any element of H . We have to show that h can be expressed as a power of $\phi(a)$. Now $h = \phi(g)$ for some $g \in G$. Since (G, \circ) is generated by a , we have

$$g = a^k$$

for some integer k . Hence

$$\phi(g) = \phi(a^k).$$

By Theorem B45(c), this gives

$$\phi(g) = (\phi(a))^k,$$

that is,

$$h = (\phi(a))^k.$$

This expresses h as a power of $\phi(a)$. Thus $(H, *)$ is cyclic, generated by $\phi(a)$. ■

You can sometimes use some of the properties of isomorphisms and isomorphic groups that you have met in this subsection and in the previous subsection to show that two particular groups are *not* isomorphic. Unfortunately there is no general, systematic procedure for showing that two groups are not isomorphic: you just have to find some means of demonstrating that they have different structures. Some suggestions are given in the strategy below.

Strategy B5

To show that two groups are not isomorphic, try any of the following methods.

- Compare their orders: if one group is finite and the other is infinite, or if they have different finite orders, then they are not isomorphic.
- Ascertain whether they are abelian or cyclic: if one group is abelian and the other is not, or if one group is cyclic and the other is not, then they are not isomorphic.
- Compare the numbers of self-inverse elements: if one group has more self-inverse elements than the other, then they are not isomorphic.
- Compare the entries in the main diagonals of their Cayley tables, if these are available. For example, count the numbers of different elements that appear: if the count is different for the two groups, then they are not isomorphic.
- Compare the numbers of elements of a particular order: if one group has more elements of this order than the other, then they are not isomorphic.

The fourth suggestion in the box above relies on the fact that the n elements (not necessarily distinct) that occur on the main diagonal of the Cayley table of a group of order n are the n elements obtained by composing each group element with itself. So rearranging the borders of the Cayley table will not change these n elements, though it may change their positions on the diagonal.

Exercise B78

In each of the following cases, show that the two groups are not isomorphic.

(a) $(\mathbb{Z}_8, +_8)$ and $(S(\triangle), \circ)$.

(b) $(\mathbb{Z}_8, +_8)$ and (U_{20}, \times_{20}) .

(You were asked to investigate some properties of the group (U_{20}, \times_{20}) in Exercise B65.)

4.4 Isomorphisms of cyclic groups

Near the end of Subsection 3.4 you saw that the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ have the same structure, namely a cyclic structure, as shown in Figure 42.

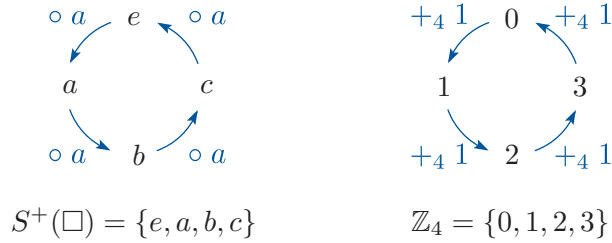


Figure 42 The cycle of powers of a in $(S^+(\square), \circ)$ and the cycle of multiples of 1 in $(\mathbb{Z}_4, +_4)$

Each power of the generator a in $(S^+(\square), \circ)$ matches up with the corresponding multiple of the generator 1 in the additive group $(\mathbb{Z}_4, +_4)$ to give the following isomorphism:

$$\begin{aligned}\phi : S^+(\square) &\longrightarrow \mathbb{Z}_4 \\ e = a^0 &\longmapsto 0 \times 1 = 0 \\ a = a^1 &\longmapsto 1 \times 1 = 1 \\ b = a^2 &\longmapsto 2 \times 1 = 2 \\ c = a^3 &\longmapsto 3 \times 1 = 3.\end{aligned}$$

This isomorphism is set out again below, with the powers in $(S^+(\square), \circ)$ and the multiples in $(\mathbb{Z}_4, +_4)$ expanded to make it clear how the elements match up:

$$\begin{aligned}\phi : S^+(\square) &\longrightarrow \mathbb{Z}_4 \\ e &\longmapsto 0 \\ a &\longmapsto 1 \\ a \circ a &\longmapsto 1 +_4 1 \\ a \circ a \circ a &\longmapsto 1 +_4 1 +_4 1.\end{aligned}$$

More generally, consider any two finite cyclic groups (G, \circ) and $(H, *)$ with the same order n . They have the same structure, as shown in Figure 43; here a and b are generators of (G, \circ) and $(H, *)$, respectively.

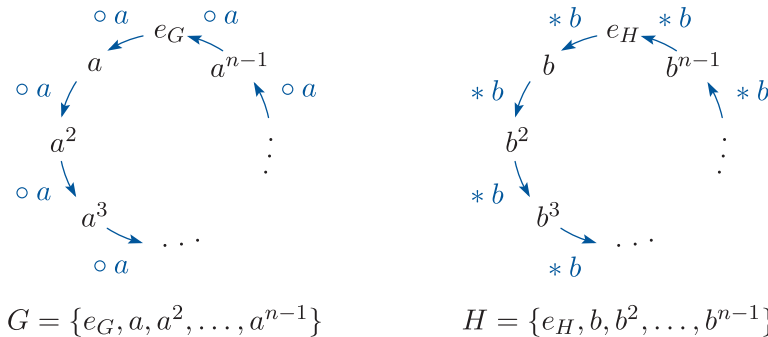


Figure 43 The cycles of powers of a generator in two cyclic groups of order n

Each power of the generator a of the first cyclic group matches up with the corresponding power of the generator b of the second group, to give the isomorphism

$$\begin{aligned}\phi : G &\longrightarrow H \\ e_G &\longmapsto e_H \\ a &\longmapsto b \\ a^2 &\longmapsto b^2 \\ a^3 &\longmapsto b^3 \\ &\vdots \\ a^{n-1} &\longmapsto b^{n-1}.\end{aligned}$$

This isomorphism can be written more concisely as

$$\begin{aligned}\phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k = 0, 1, \dots, n-1).\end{aligned}$$

That is, we have the theorem below.

Theorem B49

Let (G, \circ) and $(H, *)$ be finite cyclic groups of the same order n , generated by a and b , respectively. Then (G, \circ) and $(H, *)$ are isomorphic, and an isomorphism is given by

$$\begin{aligned}\phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k = 0, 1, \dots, n-1).\end{aligned}$$

Proof The mapping ϕ defined above is one-to-one and onto. Also, for all $a^j, a^k \in G$,

$$\phi(a^j \circ a^k) = \phi(a^{j+k}) = b^{j+k} = b^j * b^k = \phi(a^j) * \phi(a^k).$$

So ϕ is an isomorphism. ■

Since all cyclic groups of any particular order are isomorphic to each other, the notation below is sometimes useful. You have met this notation already for cyclic groups of orders 4 and 6.

Notation

The notation C_n denotes a standard, abstract cyclic group of order n . We refer to it as *the cyclic group of order n* .

Theorem B49 gives us the following strategy for finding an isomorphism from one finite cyclic group to another of the same order.

Strategy B6

To find an isomorphism between two finite cyclic groups (G, \circ) and $(H, *)$ of the same order n , do the following.

1. Find a generator a of (G, \circ) and a generator b of $(H, *)$.
2. Construct the isomorphism

$$\begin{aligned}\phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k = 0, 1, \dots, n-1).\end{aligned}$$



Keep in mind that if you want to apply Strategy B6 to two groups where either or both are *additive* cyclic groups, then you need to translate step 2 of the strategy into additive notation as appropriate. For an additive cyclic group $(G, +)$ generated by a , the power a^k becomes the multiple ka , and similarly for an additive cyclic group $(H, +)$ generated by b , the power b^k becomes the multiple kb .

You have seen that usually a cyclic group has more than one generator. By applying Strategy B6 more than once, using different generators, we can find more than one isomorphism between two finite cyclic groups of the same order.

Worked Exercise B31



Find two isomorphisms from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

Solution

 Use Strategy B6. To find one isomorphism, first find a generator of each group. Match up corresponding powers of the generators, starting by matching the identities of each group (the zeroth powers). 

The group $(\mathbb{Z}_4, +_4)$ is generated by 1; the group $(\mathbb{Z}_5^*, \times_5)$ is generated by 2 (as found in Exercise B58(c)). So an isomorphism is given by

$$\begin{array}{lll}\phi : \mathbb{Z}_4 &\longrightarrow \mathbb{Z}_5^* & \phi : \mathbb{Z}_4 &\longrightarrow \mathbb{Z}_5^* \\ 0 &\longmapsto 1 & 0 &\longmapsto 1 \\ 1 &\longmapsto 2 & \text{that is,} & 1 &\longmapsto 2 \\ 1 +_4 1 &\longmapsto 2 \times_5 2 & & 2 &\longmapsto 4 \\ 1 +_4 1 +_4 1 &\longmapsto 2 \times_5 2 \times_5 2, & & 3 &\longmapsto 3.\end{array}$$

 To find a different isomorphism, find a different generator of one of the groups. 

The group $(\mathbb{Z}_4, +_4)$ is also generated by 3, so another isomorphism is given by

$$\begin{array}{ll}
\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_5^* & \phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_5^* \\
0 \mapsto 1 & 0 \mapsto 1 \\
3 \mapsto 2 & \text{that is, } 3 \mapsto 2 \\
3 +_4 3 \mapsto 2 \times_5 2 & 2 \mapsto 4 \\
3 +_4 3 +_4 3 \mapsto 2 \times_5 2 \times_5 2, & 1 \mapsto 3.
\end{array}$$

Exercise B79

- (a) Write down the elements of the set U_9 of integers in \mathbb{Z}_9 coprime to 9. Show that the group (U_9, \times_9) is cyclic and find all its generators.
- (b) Hence find two isomorphisms $\phi : (U_9, \times_9) \longrightarrow (\mathbb{Z}_6, +_6)$.

Exercise B80

- (a) Let $G = \{1, 2, 4, 8, 9, 13, 15, 16\}$. Show that (G, \times_{17}) is a cyclic group, and find all its generators.
- (b) Let (C, \circ) be an abstract cyclic group of order 8, generated by the element x , so that

$$C = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7\}.$$

Find four isomorphisms $\phi : (G, \times_{17}) \longrightarrow (C, \circ)$.

Theorem B49 tells us in particular that every cyclic group of order n is isomorphic to the cyclic group $(\mathbb{Z}_n, +_n)$. Hence the results about $(\mathbb{Z}_n, +_n)$ that you met in Subsection 3.4 provide results about *every* cyclic group of order n . For example, you saw in Theorem B41 in Subsection 3.4 that the group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order q for each positive factor q of n , and no other subgroups. By Theorem B49 (and Theorem B47), the same is true of *every* cyclic group of order n .

Powers of generators in infinite cyclic groups can be matched up in the same way as those in finite cyclic groups, which gives the following theorem.

Theorem B50

Let (G, \circ) and $(H, *)$ be infinite cyclic groups, generated by a and b , respectively. Then (G, \circ) and $(H, *)$ are isomorphic, and an isomorphism is given by

$$\begin{array}{l}
\phi : G \longrightarrow H \\
a^k \mapsto b^k \quad (k \in \mathbb{Z}).
\end{array}$$

Proof The proof of Theorem B49 applies here also. ■

The idea of isomorphism is extremely important in group theory. As you saw above, it allows us to prove results about the structure of one group, or one family of groups, and know that these results also apply to many other groups – namely, to all groups isomorphic to the group or groups that we considered.

Summary

In this unit you studied the structures of groups. You saw that groups can have *subgroups*, and looked at some ways in which subgroups of a group can be found. You saw that the set consisting of all the powers of an element of a group is always a subgroup of the group, called the *cyclic subgroup generated* by that element. You met the idea of a *cyclic* group, which is a group that itself consists of all the powers of one of its elements, and you studied some properties of cyclic groups. You learned about the different notations used for additive and multiplicative groups. Finally, you met the powerful concept of *isomorphism*, which links groups that have the same structure and which can therefore be considered in a sense to be ‘the same group’.

Learning outcomes

After working through this unit, you should be able to:

- understand what is meant by a *subgroup*
- use the three subgroup properties to determine whether (H, \circ) is a subgroup of a group (G, \circ) , where H is a subset of the set G
- find subgroups of a symmetry group $S(F)$ by adding features to the figure F , or by fixing a feature of F
- translate results in group theory from multiplicative notation to additive notation, and vice versa
- understand what is meant by the *order* of a group element and the *cyclic subgroup generated* by a group element, and find these for group elements of reasonably small order
- understand the terms *cyclic group*, and *generator* of a cyclic group
- know that every subgroup of a cyclic group is also cyclic
- find all the subgroups and all the generators of a cyclic group of any reasonably small order, and in particular do this efficiently for $(\mathbb{Z}_n, +_n)$
- explain the meaning of the terms *isomorphic groups* and *isomorphism*
- in some cases, show that two groups are isomorphic and find an isomorphism, or show that the groups are not isomorphic
- know that any two cyclic groups of the same order are isomorphic, and find isomorphisms from one cyclic group to another of the same order
- know some basic properties of isomorphisms and isomorphic groups.

Solutions to exercises

Solution to Exercise B35

(a) We obtain a Cayley table for $\{e, s\}$ under \circ by deleting the rows and columns labelled a, b, r and t in the group table of $(S(\Delta), \circ)$:

o	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

o	e	s
e	e	s
s	s	e

We now check the four group axioms.

G1 Every element in the body of the table is in the set $\{e, s\}$, so $\{e, s\}$ is closed under function composition.

G2 Function composition is associative.

G3 The row and column labelled e repeat the table borders, so e is an identity element.

G4 We see that e and s are both self-inverse.

Hence $(\{e, s\}, \circ)$ satisfies the four group axioms, and so is a group.

The set $\{e, s\}$ is a subset of the set $S(\Delta)$, so $(\{e, s\}, \circ)$ is a subgroup of $(S(\Delta), \circ)$.

(b) We obtain a Cayley table for $\{e, b, r\}$ under \circ by deleting the rows and columns labelled by a, s and t in the group table of $(S(\Delta), \circ)$:

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

 \longrightarrow

\circ	e	b	r
e	e	b	r
b	b	a	s
r	r	t	e

We now check the group axioms.

G1 The Cayley table for $\{e, b, r\}$ contains elements other than e, b and r , so $\{e, b, r\}$ is not closed under the operation \circ . That is, axiom G1 fails.

Hence $(\{e, b, r\}, \circ)$ is not a group, and therefore it is not a subgroup of $(S(\Delta), \circ)$.

Solution to Exercise B36

We have $\{e, b, s, u\} \subseteq S(\square)$, and the binary operation \circ is the same on each set.

The Cayley table for $(\{e, b, s, u\}, \circ)$ is as follows.

\circ	e	b	s	u
e	e	b	s	u
b	b	e	u	s
s	s	u	e	b
u	u	s	b	e

We check the three subgroup properties.

SG1 Every element in the body of the table is in $\{e, b, s, u\}$, so this set is closed under function composition.

SG2 The identity element in $S(\square)$ is e , and we have $e \in \{e, b, s, u\}$.

SG3 The elements e, b, s and u are all self-inverse, so $\{e, b, s, u\}$ contains the inverse of each of its elements.

Hence $(\{e, b, s, u\}, \circ)$ satisfies the three subgroup properties, and so is a subgroup of $(S(\square), \circ)$.

Solution to Exercise B37

(a) The Cayley table for $(\{1, -1, i, -i\}, \times)$ is as follows.

\times	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(b) We have $\{1, -1, i, -i\} \subseteq \mathbb{C}^*$, and the binary operation \times is the same on each set.

We check the three subgroup properties.

SG1 Every element in the body of the table is in $\{1, -1, i, -i\}$, so this set is closed under multiplication.

SG2 The identity element in \mathbb{C}^* is 1, and $1 \in \{1, -1, i, -i\}$.

SG3 From the table, we see that the elements 1 and -1 are self-inverse, and i and $-i$ are inverses of each other, so $\{1, -1, i, -i\}$ contains the inverse of each of its elements.

Hence $(\{1, -1, i, -i\}, \times)$ satisfies the three subgroup properties, and so is a subgroup of (\mathbb{C}^*, \times) .

(The easiest way to find the inverses of i and $-i$ here is to use the Cayley table, but you could also just use arithmetic in \mathbb{C} in the usual way. For example, the multiplicative inverse of i is

$$\frac{1}{i} = \frac{1 \times (-i)}{i \times (-i)} = \frac{-i}{1} = -i.)$$

Solution to Exercise B38

We have $3\mathbb{Z} \subseteq \mathbb{Z}$, and the binary operation $+$ is the same on each set.

We show that the three subgroup properties hold.

SG1 Let $x, y \in 3\mathbb{Z}$; then $x = 3r$ and $y = 3s$, for some $r, s \in \mathbb{Z}$. Thus

$$x + y = 3r + 3s = 3(r + s).$$

Since $r + s$ is an integer, it follows that $x + y \in 3\mathbb{Z}$. Hence $3\mathbb{Z}$ is closed under addition.

SG2 The identity in $(\mathbb{Z}, +)$ is 0, and $0 = 3 \times 0 \in 3\mathbb{Z}$, so $3\mathbb{Z}$ contains the identity.

SG3 Let $x \in 3\mathbb{Z}$. Then $x = 3r$ for some $r \in \mathbb{Z}$. The inverse of $x = 3r$ in $(\mathbb{Z}, +)$ is

$$-x = -3r = 3(-r),$$

which is an element of $3\mathbb{Z}$ since $-r$ is an integer. Thus $3\mathbb{Z}$ contains the inverse of each of its elements.

Hence $(3\mathbb{Z}, +)$ satisfies the three subgroup properties, and so is a subgroup of $(\mathbb{Z}, +)$.

Solution to Exercise B39

(a) $(6\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$, by the result in the box immediately before the exercise.

(b) By the result in the box, both $(6\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are groups. Also, $6\mathbb{Z} \subseteq 2\mathbb{Z}$, since every

multiple of 6 is also a multiple of 2. So $(6\mathbb{Z}, +)$ is a subgroup of $(2\mathbb{Z}, +)$.

(Notice that there is no need to check the three subgroup properties here, because we already know that both $(6\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are groups, by the result in the box.)

(c) $5\mathbb{Z}$ is not a subset of $3\mathbb{Z}$; for example, 5 is a multiple of 5 but is not a multiple of 3. Hence $(5\mathbb{Z}, +)$ is not a subgroup of $(3\mathbb{Z}, +)$.

Solution to Exercise B40

(a) The set \mathbb{Q}^* is not a subset of \mathbb{R}^+ ; for example, $-1 \in \mathbb{Q}^*$, but $-1 \notin \mathbb{R}^+$, so $\mathbb{Q}^* \not\subseteq \mathbb{R}^+$. It follows that (\mathbb{Q}^*, \times) is not a subgroup of (\mathbb{R}^+, \times) .

(b) We have $W \subseteq \mathbb{Z}$, and the binary operation is the same on each set.

However, we have $1 \in W$, but the inverse of 1 in $(\mathbb{Z}, +)$, namely -1 , is not in W . So property SG3 fails and hence $(W, +)$ is not a subgroup of $(\mathbb{Z}, +)$.

Solution to Exercise B41

We have $H \subseteq \mathbb{Z}_{12}$, and the binary operation $+_{12}$ is the same on each set.

We show that the three subgroup properties hold.

The Cayley table for $(H, +_{12})$ is as follows.

$+_{12}$	0	3	6	9
0	0	3	6	9
3	3	6	9	0
6	6	9	0	3
9	9	0	3	6

SG1 Every element in the table is in H , so H is closed under $+_{12}$.

SG2 The identity in $(\mathbb{Z}_{12}, +_{12})$ is 0, and $0 \in H$.

SG3 From the Cayley table, we see that the inverse of each element of H is in H , as below.

Element	0	3	6	9
Inverse	0	9	6	3

Hence $(H, +_{12})$ satisfies the three subgroup properties, and so is a subgroup of $(\mathbb{Z}_{12}, +_{12})$.

Solution to Exercise B42

- (a) Property SG1 fails: $a \circ a = b$, but $b \notin H$.
 (b) Property SG1 fails: $2 \times_5 3 = 1$, but $1 \notin H$.
 (Alternatively, property SG2 fails: the identity in \mathbb{Z}_5^* is 1, but $1 \notin H$.)
 (c) Property SG3 fails: for example, the inverse of 2 in (\mathbb{R}^*, \times) is $\frac{1}{2}$, but $\frac{1}{2} \notin \mathbb{Z}^*$.

Solution to Exercise B43

(a) We show that $(X, *)$ satisfies the four group axioms.

G1 Let $(a, b), (c, d) \in X$; then $a \neq 0, b \neq 0, c \neq 0$ and $d \neq 0$. We have

$$(a, b) * (c, d) = (ac, bd).$$

This point is in \mathbb{R}^2 since $a, b, c, d \in \mathbb{R}$. Also $ac \neq 0$ because $a \neq 0$ and $c \neq 0$, and similarly $bd \neq 0$ because $b \neq 0$ and $d \neq 0$. So this point is in X . Thus X is closed under $*$.

G2 Let $(a, b), (c, d), (e, f) \in X$. We have

$$\begin{aligned} (a, b) * ((c, d) * (e, f)) \\ &= (a, b) * (ce, df) \\ &= (ace, bdf), \end{aligned}$$

and

$$\begin{aligned} ((a, b) * (c, d)) * (e, f) \\ &= (ac, bd) * (e, f) \\ &= (ace, bdf). \end{aligned}$$

The two expressions obtained are the same, so $*$ is associative on X .

G3 Suppose that (x, y) is an identity in X . Then we must have, for each $(a, b) \in X$,

$$(a, b) * (x, y) = (a, b) = (x, y) * (a, b).$$

The left-hand equation gives

$$(ax, by) = (a, b).$$

Comparing coordinates, we obtain

$$ax = a \quad \text{and} \quad by = b.$$

Since these equations must hold for all non-zero values of a and b , we must have

$$x = y = 1.$$

So the only possibility for an identity is $(1, 1)$.

Now $(1, 1)$ is in X , since it is in \mathbb{R}^2 and both its coordinates are non-zero, and for all $(a, b) \in X$, we have

$$(a, b) * (1, 1) = (a, b),$$

and

$$(1, 1) * (a, b) = (a, b).$$

So $(1, 1)$ is an identity for $*$ on X .

G4 Let $(a, b) \in X$; then $a \neq 0$ and $b \neq 0$. Suppose that (x, y) is an inverse of (a, b) . Then we must have

$$(a, b) * (x, y) = (1, 1) = (x, y) * (a, b).$$

The left-hand equation gives

$$(ax, by) = (1, 1).$$

Comparing coordinates, we obtain

$$ax = 1 \quad \text{and} \quad by = 1.$$

Since $a \neq 0$ and $b \neq 0$, these equations give

$$x = 1/a \quad \text{and} \quad y = 1/b.$$

So the only possibility for an inverse of (a, b) is $(1/a, 1/b)$.

Now $(1/a, 1/b) \in X$, since both its coordinates are non-zero, and we have

$$(a, b) * (1/a, 1/b) = (1, 1),$$

and

$$(1/a, 1/b) * (a, b) = (1, 1).$$

So $(1/a, 1/b)$ is an inverse of (a, b) . Thus every element of X has an inverse in X .

Hence $(X, *)$ satisfies the four group axioms, and so is a group.

(b) (i) We can simplify the description of the set A , as follows:

$$A = \{(a, b) \in X : a = 1\} = \{(1, b) : b \in \mathbb{R}^*\}.$$

We show that $(A, *)$ satisfies the three subgroup properties.

SG1 Let $(1, b), (1, d) \in A$; then $b \neq 0$ and $d \neq 0$. We have

$$(1, b) * (1, d) = (1, bd).$$

This point is in A because its first coordinate is 1 and its second coordinate is non-zero, since $b \neq 0$ and $d \neq 0$. Thus A is closed under $*$.

SG2 The identity in X is $(1, 1)$. This point is in A , because its first coordinate is 1 and its second coordinate is non-zero.

SG3 Let $(1, b) \in A$. By the solution to part (a), the inverse of $(1, b)$ in A is $(1/1, 1/b) = (1, 1/b)$. This point has first coordinate 1 and its second coordinate is non-zero, so it is in A . Thus A contains the inverse of each of its elements.

Hence $(A, *)$ satisfies the three subgroup properties, and so is a subgroup of $(X, *)$.

(ii) The points $(3, -1)$ and $(4, -2)$ are in B , but

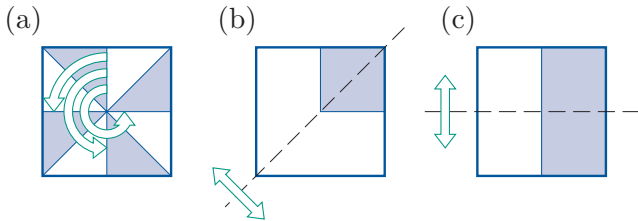
$$(3, -1) * (4, -2) = (12, 2) \notin B.$$

Thus B is not closed under $*$; that is, property SG1 fails.

Hence $(B, *)$ is not a subgroup of $(X, *)$.

Solution to Exercise B44

The non-identity symmetries of the three modified squares are shown below.



(a) The symmetry group of the modified square is $\{e, a, b, c\} = S^+(\square)$.

(Any reflection interchanges the shaded and unshaded areas.)

(b) The symmetry group of the modified square is $\{e, u\}$.

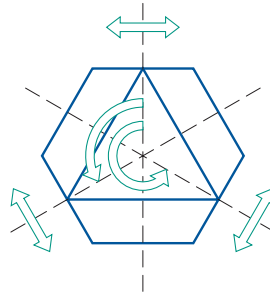
(The other elements of $S(\square)$ move the shaded square to a different corner.)

(c) The symmetry group of the modified square is $\{e, t\}$.

(The other elements of $S(\square)$ move the shaded rectangle to other parts of the square.)

Solution to Exercise B45

The non-identity symmetries of F' are shown below.



The elements of $S(F')$ are:

- the identity
- rotations through $2\pi/3$ and $4\pi/3$ about the centre
- reflections in the three axes shown above.

The other elements of $S(\square)$ do not map the triangle to itself. Thus the effect of the inscribed equilateral triangle is to restrict the symmetries of the modified hexagon to those of the triangle.

Solution to Exercise B46

The required subgroup is

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \right\}.$$

(One way to obtain these two-line symbols is to start with the subgroup in Worked Exercise B21, replace each occurrence of the symbol 3 with the symbol 4 and vice versa, and then rearrange the columns in each two-line symbol so that the numbers in the top row are in the natural order.)

Solution to Exercise B47

The required subgroup is

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \right\}.$$

(It consists of all the elements of $S(\text{tet})$ that either fix the vertices at locations 1 and 2, or interchange them.)

Solution to Exercise B48

(a) The symmetries of the modified framework prism form a subgroup of $S(F)$ whose elements are as follows.

The identity:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

The rotation through π about the vertical axis through the centre of the prism:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

The reflection in the vertical plane through locations 1 and 4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}.$$

The reflection in the vertical plane through the midpoints of the edges joining the vertices at locations 1 and 4, 2 and 5, and 3 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}.$$

Thus we obtain a subgroup of $S(F)$ of order 4 (that is, with 4 elements).

(b) Here, the symmetries of the modified framework prism are ‘essentially the same’ as those of $S(\triangle)$, so we obtain a subgroup of $S(F)$ whose elements are as follows.

The identity:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

The rotations through $2\pi/3$ and $4\pi/3$ about the horizontal axis of symmetry:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix}.$$

The reflection in the vertical plane through locations 1 and 4, and the midpoints of the edges joining the vertices at locations 2 and 3, and 5 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}.$$

The reflection in the plane through locations 2 and 5, and the midpoints of the edges joining the vertices at locations 1 and 3, and 4 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}.$$

The reflection in the plane through locations 3 and 6, and the midpoints of the edges joining the vertices at locations 1 and 2, and 4 and 5:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{pmatrix}.$$

Thus we obtain a subgroup of $S(F)$ of order 6.

(c) The symmetries of the modified framework prism, with the vertices at locations 1 and 4 fixed, form a subgroup of $S(F)$ whose elements are as follows.

The identity:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

The reflection in the plane through locations 1 and 4, and the midpoints of the edges joining the vertices at locations 2 and 3, and 5 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}.$$

Thus we obtain a subgroup of $S(F)$ of order 2.

Solution to Exercise B49

(a) $a^0 = e$,

$$a^1 = a,$$

$$a^2 = a \circ a$$

$$= b,$$

$$a^3 = a \circ a \circ a$$

$$= b \circ a$$

$$= c,$$

$$a^4 = a \circ a \circ a \circ a$$

$$= c \circ a$$

$$= e,$$

$$a^5 = a \circ a \circ a \circ a \circ a$$

$$= e \circ a$$

$$= a.$$

$$\begin{aligned}
\text{(b)} \quad a^{-1} &= c, \\
a^{-2} &= a^{-1} \circ a^{-1} \\
&= c \circ c \\
&= b, \\
a^{-3} &= a^{-1} \circ a^{-1} \circ a^{-1} \\
&= b \circ c \\
&= a, \\
a^{-4} &= a^{-1} \circ a^{-1} \circ a^{-1} \circ a^{-1} \\
&= a \circ c \\
&= e, \\
a^{-5} &= a^{-1} \circ a^{-1} \circ a^{-1} \circ a^{-1} \circ a^{-1} \\
&= e \circ c \\
&= c.
\end{aligned}$$

$$\begin{aligned}
\text{(c)} \quad b^0 &= e, \\
b^1 &= b, \\
b^2 &= b \circ b \\
&= e, \\
b^3 &= b \circ b \circ b \\
&= e \circ b \\
&= b \\
b^4 &= b \circ b \circ b \circ b \\
&= b \circ b \\
&= e.
\end{aligned}$$

$$\begin{aligned}
\text{(d)} \quad b^{-1} &= b, \\
b^{-2} &= b^{-1} \circ b^{-1} \\
&= b \circ b \\
&= e, \\
b^{-3} &= b^{-1} \circ b^{-1} \circ b^{-1} \\
&= e \circ b \\
&= b.
\end{aligned}$$

$$\begin{aligned}
\text{(e)} \quad r^0 &= e, \\
r^1 &= r, \\
r^2 &= r \circ r \\
&= e, \\
r^3 &= r \circ r \circ r \\
&= e \circ r \\
&= r \\
r^4 &= r \circ r \circ r \circ r \\
&= r \circ r \\
&= e.
\end{aligned}$$

Solution to Exercise B50

We have

$$\begin{aligned}
x^2 \circ (x^{-1})^2 &= x \circ x \circ x^{-1} \circ x^{-1} \\
&= x \circ e \circ x^{-1} \\
&= x \circ x^{-1} \\
&= e,
\end{aligned}$$

and similarly,

$$\begin{aligned}
(x^{-1})^2 \circ x^2 &= x^{-1} \circ x^{-1} \circ x \circ x \\
&= x^{-1} \circ e \circ x \\
&= x^{-1} \circ x \\
&= e.
\end{aligned}$$

Thus $(x^{-1})^2$ is an inverse of x^2 , and, since the inverse of any group element is unique, it follows that $(x^{-1})^2$ is the inverse of x^2 .

Solution to Exercise B51

(a) $x^0 = e$ translates to

$$0x = 0.$$

(b) $x \circ x^{-1} = e$ translates to

$$x + (-x) = 0.$$

(c) $x \circ x^2 = x^3$ translates to

$$x + 2x = 3x.$$

(d) $(x^{-1})^{-1} = x$ translates to

$$-(-x) = x.$$

(e) $e \circ x = x$ translates to

$$0 + x = x.$$

(f) $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$ translates to

$$-(x + y) = (-y) + (-x),$$

or alternatively, since $(G, +)$ is abelian,

$$-(x + y) = (-x) + (-y).$$

Solution to Exercise B52

(a) The element c in $S(\square)$ has order 4, since the smallest (positive) number of times that we need to apply c to bring the square back to its starting position is 4.

(b) The element r in $S(\square)$ has order 2, since the smallest (positive) number of times that we need to apply r to bring the square back to its starting position is 2.

(c) The smallest positive value of n such that

$$\underbrace{1 +_6 1 +_6 \cdots +_6 1}_{n \text{ copies of } 1} = 0$$

is 6, so 1 in $(\mathbb{Z}_6, +_6)$ has order 6.

(d) The smallest positive value of n such that

$$\underbrace{2 +_6 2 +_6 \cdots +_6 2}_{n \text{ copies of } 2} = 0$$

is 3, so 2 in $(\mathbb{Z}_6, +_6)$ has order 3.

(e) In (U_9, \times_9) we have

$$5^2 = 5 \times_9 5 = 7,$$

$$5^3 = 5^2 \times_9 5 = 7 \times_9 5 = 8,$$

$$5^4 = 5^3 \times_9 5 = 8 \times_9 5 = 4,$$

$$5^5 = 5^4 \times_9 5 = 4 \times_9 5 = 2,$$

$$5^6 = 5^5 \times_9 5 = 2 \times_9 5 = 1.$$

So the element 5 in (U_9, \times_9) has order 6.

(f) In (U_{10}, \times_{10}) we have

$$9^2 = 9 \times_{10} 9 = 1.$$

So the element 9 in (U_{10}, \times_{10}) has order 2.

(g) No positive multiple of 1 in $(\mathbb{Z}, +)$ is equal to the identity element 0, so 1 in $(\mathbb{Z}, +)$ has infinite order.

(h) We have

$$i^2 = i \times i = -1,$$

$$i^3 = i^2 \times i = (-1) \times i = -i,$$

$$i^4 = i^3 \times i = (-i) \times i = 1.$$

So the element i in (\mathbb{C}^*, \times) has order 4.

Solution to Exercise B53

The identity element 0 of $(\mathbb{Z}, +)$ has order 1, because $1 \times 0 = 0$ and so the smallest positive integer n such that $n0 = 0$ is 1.

All other elements of $(\mathbb{Z}, +)$ have infinite order, because there is no positive multiple of such an element that is equal to 0.

Solution to Exercise B54

Let x be an element of infinite order in the group (G, \circ) . We will prove by contradiction that all the powers

$$\dots, x^{-2}, x^{-1}, e, x, x^2, \dots$$

of x are distinct. Suppose that these powers are *not* distinct. Then

$$x^s = x^t,$$

for some integers s and t with $s < t$. Composing each side of this equation on the right with $(x^s)^{-1}$ gives

$$x^s \circ (x^s)^{-1} = x^t \circ (x^s)^{-1}.$$

Simplifying (using the index laws on the right-hand side) gives

$$e = x^{t-s}.$$

Now $t - s > 0$, so there is a positive power of x that is equal to e . This is a contradiction, since x has infinite order. Thus all the powers of x in the list above are distinct.

Solution to Exercise B55

(a) The identity element e of $S(\triangle)$ has order 1.

For the element a , we have

$$a^2 = a \circ a = b,$$

$$a^3 = a^2 \circ a = b \circ a = e.$$

Thus a has order 3. Hence b , the inverse of a , also has order 3.

All the other elements of $S(\triangle)$ are self-inverse and hence have order 2.

In summary, the orders of the elements of $S(\triangle)$ are as follows.

Element	e	a	b	r	s	t
Order	1	3	3	2	2	2

(b) The identity element e of $S(\square)$ has order 1, and the remaining elements a , r and s are all self-inverse and hence all have order 2. In summary, the orders of the elements are as follows.

Element	e	a	r	s
Order	1	2	2	2

(c) The Cayley table for $(\mathbb{Z}_5^*, \times_5)$ is as follows.

\times_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The identity element 1 has order 1.

For the element 2, we have

$$\begin{aligned} 2^2 &= 2 \times_5 2 = 4, \\ 2^3 &= 2^2 \times_5 2 = 4 \times_5 2 = 3, \\ 2^4 &= 2^3 \times_5 2 = 3 \times_5 2 = 1. \end{aligned}$$

Thus 2 has order 4. Hence 3, the inverse of 2, also has order 4.

The element 4 is self-inverse, so it has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_5^*, \times_5)$ are as follows.

Element	1	2	3	4
Order	1	4	4	2

(d) The identity element 0 of $(\mathbb{Z}_8, +_8)$ has order 1.

For the element 1, we have

$$\begin{aligned} 1 +_8 1 &= 2 \\ 1 +_8 1 +_8 1 &= 3 \\ 1 +_8 1 +_8 1 +_8 1 &= 4 \\ &\vdots \\ \underbrace{1 +_8 1 +_8 \cdots +_8 1}_{7 \text{ copies of } 1} &= 7 \\ \underbrace{1 +_8 1 +_8 \cdots +_8 1}_{8 \text{ copies of } 1} &= 0 \end{aligned}$$

Thus 1 has order 8. Hence 7, the inverse of 1, also has order 8.

For the element 2, we have

$$\begin{aligned} 2 +_8 2 &= 4 \\ 2 +_8 2 +_8 2 &= 6 \\ 2 +_8 2 +_8 2 +_8 2 &= 0 \end{aligned}$$

Thus 2 has order 4. Hence 6, the inverse of 2, also has order 4.

For the element 3, we have

$$\begin{aligned} 3 +_8 3 &= 6 \\ 3 +_8 3 +_8 3 &= 1 \\ 3 +_8 3 +_8 3 +_8 3 &= 4 \\ 3 +_8 3 +_8 3 +_8 3 +_8 3 &= 7 \\ 3 +_8 3 +_8 3 +_8 3 +_8 3 +_8 3 &= 2 \\ \underbrace{3 +_8 3 +_8 \cdots +_8 3}_{7 \text{ copies of } 3} &= 5 \\ \underbrace{3 +_8 3 +_8 \cdots +_8 3}_{8 \text{ copies of } 3} &= 0 \end{aligned}$$

Thus 3 has order 8. Hence 5, the inverse of 3, also has order 8.

Finally, for the element 4, we have

$$4 +_8 4 = 0$$

Thus 4 has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_8, +_8)$ are as follows.

Element	0	1	2	3	4	5	6	7
Order	1	8	4	8	2	8	4	8

Solution to Exercise B56

(a) We have $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. (Recall that U_{20} is the set of all integers in \mathbb{Z}_{20} that are coprime to 20.)

The order of the identity element 1 is 1.

The powers of 3 are

$$\dots, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, \dots$$

So 3 has order 4.

The element immediately before the identity element 1 in the cycle of powers of 3 is 7, so 7 is the inverse of 3 and hence it also has order 4. Also, the cycle shows that the powers of $9 = 3^2$ are

$$\dots, 1, 9, 1, 9, 1, 9, \dots,$$

so 9 has order 2.

The powers of 11 are

$$\dots, 1, 11, 1, 11, 1, 11, \dots,$$

so 11 has order 2.

The powers of 13 are

$$\dots, 1, 13, 9, 17, 1, 13, 9, 17, 1, 13, 9, 17, \dots$$

So 13 has order 4, and 17 is the inverse of 13 and also has order 4.

Finally, the powers of 19 are

$$\dots, 1, 19, 1, 19, 1, 19, \dots$$

so 19 has order 2.

In summary, the orders of the elements of (U_{20}, \times_{20}) are as follows.

Element	1	3	7	9	11	13	17	19
Order	1	4	4	2	2	4	4	2

(b) We have $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

The order of the identity element 0 is 1.

The multiples of 1 are

$$\dots, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0, 1, 2, 3, \dots$$

So 1 has order 12. Hence 11, the inverse of 1, also has order 12.

The multiples of 2 are

$$\dots, 0, 2, 4, 6, 8, 10, 0, 2, 4, 6, 8, 10, \dots$$

So 2 has order 6, and 10, the inverse of 2, also has order 6.

The multiples of 3 are

$$\dots, 0, 3, 6, 9, 0, 3, 6, 9, \dots$$

So 3 has order 4, and 9, the inverse of 3, also has order 4.

The multiples of 4 are

$$\dots, 0, 4, 8, 0, 4, 8, \dots$$

So 4 has order 3, and 8, the inverse of 4, also has order 3.

The multiples of 5 are

$$\dots, 0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0, 5, 10, 3, \dots$$

So 5 has order 12, and 7, the inverse of 5, also has order 12.

The multiples of 6 are

$$\dots, 0, 6, 0, 6, 0, 6, \dots$$

So 6 has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_{12}, +_{12})$ are as follows.

Element	0	1	2	3	4	5	6	7	8	9	10	11
Order	1	12	6	4	3	12	2	12	3	4	6	12

Solution to Exercise B57

(a) In $S(\triangle)$, the powers of a repeatedly cycle through the values e, a, b , so

$$\langle a \rangle = \{e, a, b\}.$$

(b) In $(\mathbb{Z}_7^*, \times_7)$, we have

$$3^1 = 3,$$

$$3^2 = 3 \times_7 3 = 2,$$

$$3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6,$$

$$3^4 = 3^3 \times_7 3 = 6 \times_7 3 = 4,$$

$$3^5 = 3^4 \times_7 3 = 4 \times_7 3 = 5,$$

$$3^6 = 3^5 \times_7 3 = 5 \times_7 3 = 1,$$

so

$$\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7^*.$$

(So the subset of \mathbb{Z}_7^* generated by 3 is the whole of \mathbb{Z}_7^* . We will look in more detail at groups and group elements for which this happens later in this section.)

(c) In $(\mathbb{Z}, +)$, we have

$$\begin{aligned} \langle 2 \rangle &= \{2k : k \in \mathbb{Z}\} \\ &= \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}. \end{aligned}$$

Solution to Exercise B58

We can use the cycles of powers/multiples, and self-inverse elements, found in the solution to Exercise B55. We can cut down the working by using the fact that an element and its inverse generate the same cyclic subgroup.

(a) In $S(\triangle)$ we have

$$\begin{aligned}\langle e \rangle &= \{e\}, \\ \langle a \rangle &= \{e, a, b\}, \\ \langle b \rangle &= \{e, a, b\}, \\ \langle r \rangle &= \{e, r\}, \\ \langle s \rangle &= \{e, s\}, \\ \langle t \rangle &= \{e, t\}.\end{aligned}$$

(b) In $S(\square)$ we have

$$\begin{aligned}\langle e \rangle &= \{e\}, \\ \langle a \rangle &= \{e, a\}, \\ \langle r \rangle &= \{e, r\}, \\ \langle s \rangle &= \{e, s\}.\end{aligned}$$

(c) In $(\mathbb{Z}_5^*, \times_5)$ we have

$$\begin{aligned}\langle 1 \rangle &= \{1\}, \\ \langle 2 \rangle &= \{1, 2, 3, 4\} = \mathbb{Z}_5^*, \\ \langle 3 \rangle &= \{1, 2, 3, 4\} = \mathbb{Z}_5^*, \\ \langle 4 \rangle &= \{1, 4\}.\end{aligned}$$

(d) In $(\mathbb{Z}_8, +_8)$ we have

$$\begin{aligned}\langle 0 \rangle &= \{0\}, \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8, \\ \langle 2 \rangle &= \{0, 2, 4, 6\}, \\ \langle 3 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8, \\ \langle 4 \rangle &= \{0, 4\}, \\ \langle 5 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8, \\ \langle 6 \rangle &= \{0, 2, 4, 6\}, \\ \langle 7 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8.\end{aligned}$$

Solution to Exercise B59

(a) $r_{\pi/4}$ has order 8, since its powers $r_{\pi/4}, r_{\pi/4}^2, \dots, r_{\pi/4}^8$ in order are

$$r_{\pi/4}, r_{\pi/2}, r_{3\pi/4}, r_{\pi}, r_{5\pi/4}, r_{3\pi/2}, r_{7\pi/4}, r_0.$$

(Remember that $r_{2\pi} = r_0$, and that r_0 is the identity element.)

Hence $\langle r_{\pi/4} \rangle$ has order 8.

(b) $r_{\pi/3}$ has order 6, since its powers $r_{\pi/3}, r_{\pi/3}^2, \dots, r_{\pi/3}^6$ in order are

$$r_{\pi/3}, r_{2\pi/3}, r_{\pi}, r_{4\pi/3}, r_{5\pi/3}, r_0.$$

Hence $\langle r_{\pi/3} \rangle$ has order 6.

(c) $r_{2\pi/7}$ has order 7, since its powers $r_{2\pi/7}, r_{2\pi/7}^2, \dots, r_{2\pi/7}^7$ in order are

$$r_{2\pi/7}, r_{4\pi/7}, r_{6\pi/7}, r_{8\pi/7}, r_{10\pi/7}, r_{12\pi/7}, r_0.$$

Hence $\langle r_{2\pi/7} \rangle$ has order 7.

(d) r_2 has infinite order. Its powers r_2, r_2^2, r_2^3, \dots in order are

$$r_2, r_4, r_6, r_8, \dots$$

Since π is irrational, no suffix is a multiple of 2π , so there is no positive integer n such that $r_2^n = r_0$. Hence $\langle r_2 \rangle$ has infinite order.

Solution to Exercise B60

We use the orders of the elements, found in Exercise B55.

(a) $S(\triangle)$ is not cyclic, because it has order 6 but does not contain an element of order 6.

(b) $S(\square)$ is not cyclic, because it has order 4 but does not contain an element of order 4.

(c) $(\mathbb{Z}_5^*, \times_5)$ is cyclic. It has order 4 and contains two elements, namely 2 and 3, of order 4.

(d) $(\mathbb{Z}_8, +_8)$ is cyclic. It has order 8 and contains four elements, namely 1, 3, 5 and 7, of order 8.

Solution to Exercise B61

Let a be a generator of (G, \circ) . Let $g, h \in G$; then $g = a^j$ and $h = a^k$ for some $j, k \in \mathbb{Z}$. Hence

$$\begin{aligned}g \circ h &= a^j \circ a^k \\ &= a^{j+k} \\ &= a^{k+j} \\ &= a^k \circ a^j \\ &= h \circ g.\end{aligned}$$

This shows that (G, \circ) is abelian.

Solution to Exercise B62

(a) Since $(\mathbb{Z}_5^*, \times_5)$ is cyclic, all its subgroups are cyclic. From Exercise B58(c), for $(\mathbb{Z}_5^*, \times_5)$ we have

$$\begin{aligned}\langle 1 \rangle &= \{1\}, \\ \langle 2 \rangle &= \{1, 2, 3, 4\} = \mathbb{Z}_5^*, \\ \langle 3 \rangle &= \{1, 2, 3, 4\} = \mathbb{Z}_5^*, \\ \langle 4 \rangle &= \{1, 4\}.\end{aligned}$$

So the distinct subgroups of $(\mathbb{Z}_5^*, \times_5)$ are

$$\{1\}, \quad \{1, 4\}, \quad \mathbb{Z}_5^*.$$

(b) Since $(\mathbb{Z}_8, +_8)$ is cyclic, all its subgroups are cyclic. From Exercise B58(d), for $(\mathbb{Z}_8, +_8)$ we have

$$\begin{aligned}\langle 0 \rangle &= \{0\}, \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8, \\ \langle 2 \rangle &= \{0, 2, 4, 6\}, \\ \langle 3 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8, \\ \langle 4 \rangle &= \{0, 4\}, \\ \langle 5 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8, \\ \langle 6 \rangle &= \{0, 2, 4, 6\}, \\ \langle 7 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8.\end{aligned}$$

So the distinct subgroups of $(\mathbb{Z}_8, +_8)$ are

$$\{0\}, \quad \{0, 4\}, \quad \{0, 2, 4, 6\}, \quad \mathbb{Z}_8.$$

Solution to Exercise B63

The generators of $(\mathbb{Z}_8, +_8)$ are 1, 3, 5 and 7.

Solution to Exercise B64

(a) $U_{18} = \{1, 5, 7, 11, 13, 17\}$.

(b) We find the cyclic subgroup generated by each element of (U_{18}, \times_{18}) :

$$\begin{aligned}\langle 1 \rangle &= \{1\}, \\ \langle 5 \rangle &= \{1, 5, 7, 17, 13, 11\} = U_{18} = \langle 5^{-1} \rangle = \langle 11 \rangle, \\ \langle 7 \rangle &= \{1, 7, 13\} = \langle 7^{-1} \rangle = \langle 13 \rangle, \\ \langle 17 \rangle &= \{1, 17\}.\end{aligned}$$

(c) Since the element 5, for example, of (U_{18}, \times_{18}) generates the whole group, (U_{18}, \times_{18}) is cyclic.

Its generators are 5 and 11.

Solution to Exercise B65

We have

$$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\},$$

so (U_{20}, \times_{20}) has order 8.

However, the solution to Exercise B56(a) shows that (U_{20}, \times_{20}) does not contain an element of order 8. Therefore (U_{20}, \times_{20}) is not cyclic.

Solution to Exercise B66

By the solution to Exercise B64, the group (U_{18}, \times_{18}) is cyclic, so all its subgroups are cyclic. Hence its subgroups are those found in the solution to Exercise B64:

$$\{1\}, \quad \{1, 17\}, \quad \{1, 7, 13\}, \quad U_{18}.$$

Solution to Exercise B67

The Cayley table for $(\{1, 9, 11, 19\}, \times_{20})$ is as follows.

\times_{20}	1	9	11	19
1	1	9	11	19
9	9	1	19	11
11	11	19	1	9
19	19	11	9	1

We show that the three subgroup properties hold.

SG1 All the elements in the body of the table are in $\{1, 9, 11, 19\}$, so $\{1, 9, 11, 19\}$ is closed under \times_{20} .

SG2 The identity element of (U_{20}, \times_{20}) is 1, and $1 \in \{1, 9, 11, 19\}$.

SG3 Each element in $\{1, 9, 11, 19\}$ is self-inverse, so $\{1, 9, 11, 19\}$ contains the inverse of each of its elements.

Hence $(\{1, 9, 11, 19\}, \times_{20})$ satisfies the three subgroup properties, and so is a subgroup.

Finally, $(\{1, 9, 11, 19\}, \times_{20})$ is not cyclic: each element is self-inverse, so no element generates the whole subgroup $\{1, 9, 11, 19\}$.

Solution to Exercise B68

The identity element 0 has order 1.

The multiples of 1 in $(\mathbb{Z}_5, +_5)$ are

$$\dots, 0, 1, 2, 3, 4, 0, \dots$$

So 1 has order 5, and 4, the inverse of 1, also has order 5.

The multiples of 2 in $(\mathbb{Z}_5, +_5)$ are

$$\dots, 0, 2, 4, 1, 3, 0, \dots$$

So 2 has order 5, and 3, the inverse of 2, also has order 5.

In summary, the orders of the elements of $(\mathbb{Z}_5, +_5)$ are as follows.

Element	0	1	2	3	4
Order	1	5	5	5	5

Solution to Exercise B69

(a) The order of the identity element 0 in $(\mathbb{Z}_6, +_6)$ is 1.

The HCF of 1 and 6 is 1, so the order of 1 is $6/1 = 6$.

The HCF of 2 and 6 is 2, so the order of 2 is $6/2 = 3$.

The HCF of 3 and 6 is 3, so the order of 3 is $6/3 = 2$.

The HCF of 4 and 6 is 2, so the order of 4 is $6/2 = 3$.

The HCF of 5 and 6 is 1, so the order of 5 is $6/1 = 6$.

In summary, the orders of the elements of $(\mathbb{Z}_6, +_6)$ are as follows.

Element	0	1	2	3	4	5
Order	1	6	3	2	3	6

This agrees with the values in the table at the start of this subsection.

(b) The order of the identity element 0 in $(\mathbb{Z}_5, +_5)$ is 1.

All other elements are coprime to 5 and hence the HCF of each of these elements and 5 is 1. Hence all other elements have order 5.

In summary, the orders of the elements of $(\mathbb{Z}_5, +_5)$ are as follows.

Element	0	1	2	3	4
Order	1	5	5	5	5

This agrees with the solution to Exercise B68.

Solution to Exercise B70

(a) The generators of $(\mathbb{Z}_7, +_7)$ are 1, 2, 3, 4, 5 and 6 (all the non-zero elements of \mathbb{Z}_7).

(b) The generators of $(\mathbb{Z}_{10}, +_{10})$ are 1, 3, 7 and 9.

Solution to Exercise B71

(a) By Theorem B41, $(\mathbb{Z}_{12}, +_{12})$ has six subgroups, with orders 1, 2, 3, 4, 6 and 12 (the factors of 12):

$$\begin{aligned} \langle 0 \rangle &= \{0\}, \\ \langle 6 \rangle &= \{0, 6\}, \\ \langle 4 \rangle &= \{0, 4, 8\}, \\ \langle 3 \rangle &= \{0, 3, 6, 9\}, \\ \langle 2 \rangle &= \{0, 2, 4, 6, 8, 10\}, \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \mathbb{Z}_{12}. \end{aligned}$$

(b) By Theorem B41, $(\mathbb{Z}_9, +_9)$ has three subgroups, with orders 1, 3 and 9 (the factors of 9):

$$\begin{aligned} \langle 0 \rangle &= \{0\}, \\ \langle 3 \rangle &= \{0, 3, 6\}, \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \mathbb{Z}_9. \end{aligned}$$

(c) By Theorem B41, $(\mathbb{Z}_{11}, +_{11})$ has two subgroups, with orders 1 and 11 (the factors of 11):

$$\begin{aligned} \langle 0 \rangle &= \{0\}, \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = \mathbb{Z}_{11}. \end{aligned}$$

Solution to Exercise B72

(a) A suitable matching is

$$\begin{array}{cccc} e & a & b & c \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 4 & 3 \end{array}.$$

(b) A suitable matching is

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 4 & 3 \end{array}$$

(where the elements of $(\mathbb{Z}_4, +_4)$ are on the top row and the elements of $(\mathbb{Z}_5^*, \times_5)$ are on the bottom row).

Solution to Exercise B73

(a) The Cayley table of (U_{12}, \times_{12}) is as follows.

\times_{12}	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

It has the same pattern as the Cayley table of $(S(\square), \circ)$ (in particular, all four of its elements are self-inverse). So (U_{12}, \times_{12}) has the same structure as $(S(\square), \circ)$.

(b) The Cayley table of (U_{10}, \times_{10}) is as follows.

\times_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Swapping 7 and 9 in the borders of the table gives the following table.

\times_{10}	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

It has the same pattern as the Cayley table of $(\mathbb{Z}_4, +_4)$ (in particular, it has exactly two self-inverse elements). So (U_{10}, \times_{10}) has the same structure as $(\mathbb{Z}_4, +_4)$.

Solution to Exercise B74

(a) An isomorphism is

$$\begin{aligned}\phi : S(\square) &\longrightarrow U_{12} \\ e &\longmapsto 1 \\ a &\longmapsto 5 \\ r &\longmapsto 7 \\ s &\longmapsto 11.\end{aligned}$$

(There are other possibilities; in fact any one-to-one and onto mapping ϕ that maps e to 1 will do.)

(b) An isomorphism is

$$\begin{aligned}\phi : \mathbb{Z}_4 &\longrightarrow U_{10} \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 3 \\ 2 &\longmapsto 9 \\ 3 &\longmapsto 7.\end{aligned}$$

(There is one other possibility, namely

$$\begin{aligned}\phi : \mathbb{Z}_4 &\longrightarrow U_{10} \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 7 \\ 2 &\longmapsto 9 \\ 3 &\longmapsto 3.)\end{aligned}$$

Solution to Exercise B75

We must show that ϕ is one-to-one and onto, and that for all $m, n \in \mathbb{Z}$,

$$\phi(m+n) = \phi(m) + \phi(n).$$

To check that ϕ is one-to-one, let $m, n \in \mathbb{Z}$ and suppose that $\phi(m) = \phi(n)$; that is,

$$6m = 6n.$$

Then $m = n$. Thus ϕ is one-to-one.

Also, ϕ is onto because each element $6n \in 6\mathbb{Z}$ is the image under ϕ of the element $n \in \mathbb{Z}$.

Finally, for all $m, n \in \mathbb{Z}$,

$$\phi(m+n) = 6(m+n) = 6m + 6n = \phi(m) + \phi(n).$$

Hence ϕ is an isomorphism, so $(\mathbb{Z}, +) \cong (6\mathbb{Z}, +)$.

Solution to Exercise B76

We have $U_{12} = \{1, 5, 7, 11\}$, so (U_{12}, \times_{12}) is a group of order 4. Also,

$$\begin{aligned}1 \times_{12} 1 &= 1, \\ 5 \times_{12} 5 &= 1, \\ 7 \times_{12} 7 &= 1, \\ 11 \times_{12} 11 &= 1,\end{aligned}$$

so all four elements of (U_{12}, \times_{12}) are self-inverse. Hence (U_{12}, \times_{12}) is isomorphic to the Klein four-group V .

Unit B2 Subgroups and isomorphisms

The group $(S(\square), \circ)$ also has order 4 and all four of its elements are self-inverse (since its elements are the identity, two reflections and the rotation through π). Hence it is also isomorphic to V .

Since both groups are isomorphic to V , they are isomorphic to each other.

Solution to Exercise B77

We have

$$\begin{aligned}\phi(g^3) &= \phi(g^2 \circ g) \\ &= \phi(g^2) * \phi(g) \\ &\quad (\text{since } \phi \text{ is an isomorphism}) \\ &= (\phi(g))^2 * \phi(g) \quad (\text{by equation (6)}) \\ &= \phi(g)^3.\end{aligned}$$

Solution to Exercise B78

(a) $(\mathbb{Z}_8, +_8)$ has order 8 and $(S(\triangle), \circ)$ has order 6, so these groups are not isomorphic.

(b) The two groups both have order 8, since $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. However, $(\mathbb{Z}_8 +_8)$ is cyclic, but (U_{20}, \times_{20}) is not, as determined in the solution to Exercise B65. Hence these groups are not isomorphic.

Solution to Exercise B79

(a) We have

$$U_9 = \{1, 2, 4, 5, 7, 8\}.$$

The cyclic subgroups of (U_9, \times_9) are

$$\begin{aligned}\langle 1 \rangle &= \{1\}, \\ \langle 2 \rangle &= \{1, 2, 4, 8, 7, 5\}, \\ \langle 4 \rangle &= \{1, 4, 7\}, \\ \langle 5 \rangle &= \{1, 5, 7, 8, 4, 2\}, \\ \langle 7 \rangle &= \{1, 7, 4\}, \\ \langle 8 \rangle &= \{1, 8\}.\end{aligned}$$

Thus (U_9, \times_9) is cyclic, and its generators are 2 and 5.

(It is not necessary to calculate the elements of $\langle 5 \rangle$ and $\langle 7 \rangle$, because

$$\langle 2 \rangle = \langle 2^{-1} \rangle = \langle 5 \rangle \quad \text{and} \quad \langle 4 \rangle = \langle 4^{-1} \rangle = \langle 7 \rangle.$$

However, you may prefer to use this as a check, rather than as a shortcut.)

(b) The group $(\mathbb{Z}_6, +_6)$ is generated by 1.

Following Strategy B6, that is, mapping a generator to a generator, we obtain two possible isomorphisms:

$$\begin{array}{ll}\phi_1 : U_9 \longrightarrow \mathbb{Z}_6 & \phi_2 : U_9 \longrightarrow \mathbb{Z}_6 \\ 2^0 = 1 \mapsto 0 \times 1 = 0 & 5^0 = 1 \mapsto 0 \times 1 = 0 \\ 2^1 = 2 \mapsto 1 \times 1 = 1 & 5^1 = 5 \mapsto 1 \times 1 = 1 \\ 2^2 = 4 \mapsto 2 \times 1 = 2 & 5^2 = 7 \mapsto 2 \times 1 = 2 \\ 2^3 = 8 \mapsto 3 \times 1 = 3 & 5^3 = 8 \mapsto 3 \times 1 = 3 \\ 2^4 = 7 \mapsto 4 \times 1 = 4 & 5^4 = 4 \mapsto 4 \times 1 = 4 \\ 2^5 = 5 \mapsto 5 \times 1 = 5 & 5^5 = 2 \mapsto 5 \times 1 = 5.\end{array}$$

We can write these more simply as

$$\begin{array}{ll}\phi_1 : U_9 \longrightarrow \mathbb{Z}_6 & \phi_2 : U_9 \longrightarrow \mathbb{Z}_6 \\ 1 \mapsto 0 & 1 \mapsto 0 \\ 2 \mapsto 1 & 2 \mapsto 5 \\ 4 \mapsto 2 & 4 \mapsto 4 \\ 5 \mapsto 5 & 5 \mapsto 1 \\ 7 \mapsto 4 & 7 \mapsto 2 \\ 8 \mapsto 3, & 8 \mapsto 3.\end{array}$$

(Note that although there is one other generator of $(\mathbb{Z}_6, +_6)$, namely 5, mapping the generators 2 and 5 of (U_9, \times_9) in turn to 5 results in the same isomorphisms ϕ_1 and ϕ_2 as above. So ϕ_1 and ϕ_2 are the only isomorphisms from (U_9, \times_9) to $(\mathbb{Z}_6, +_6)$.)

Solution to Exercise B80

(a) The cyclic subgroups of (U_{17}, \times_{17}) generated by the elements of G are

$$\begin{aligned}\langle 1 \rangle &= \{1\}, \\ \langle 2 \rangle &= \{1, 2, 4, 8, 16, 15, 13, 9\} = \langle 2^{-1} \rangle = \langle 9 \rangle, \\ \langle 4 \rangle &= \{1, 4, 16, 13\} = \langle 4^{-1} \rangle = \langle 13 \rangle, \\ \langle 8 \rangle &= \{1, 8, 13, 2, 16, 9, 4, 15\} = \langle 8^{-1} \rangle = \langle 15 \rangle, \\ \langle 16 \rangle &= \{1, 16\}.\end{aligned}$$

Thus

$$G = \langle 2 \rangle = \langle 9 \rangle = \langle 8 \rangle = \langle 15 \rangle,$$

and it follows that G is a cyclic group under \times_{17} , with generators 2, 8, 9 and 15.

(b) The group C is generated by x .

Following Strategy B6, that is, mapping a generator to a generator, we obtain the four isomorphisms $\phi: G \rightarrow C$ given below. These correspond to

$$2 \mapsto x, \quad 8 \mapsto x, \quad 9 \mapsto x \quad \text{and} \quad 15 \mapsto x,$$

respectively.

$1 \mapsto e$	$1 \mapsto e$	$1 \mapsto e$	$1 \mapsto e$
$2 \mapsto x$	$2 \mapsto x^3$	$2 \mapsto x^7$	$2 \mapsto x^5$
$4 \mapsto x^2$	$4 \mapsto x^6$	$4 \mapsto x^6$	$4 \mapsto x^2$
$8 \mapsto x^3$	$8 \mapsto x$	$8 \mapsto x^5$	$8 \mapsto x^7$
$9 \mapsto x^7$	$9 \mapsto x^5$	$9 \mapsto x$	$9 \mapsto x^3$
$13 \mapsto x^6$	$13 \mapsto x^2$	$13 \mapsto x^2$	$13 \mapsto x^6$
$15 \mapsto x^5$	$15 \mapsto x^7$	$15 \mapsto x^3$	$15 \mapsto x$
$16 \mapsto x^4$	$16 \mapsto x^4$	$16 \mapsto x^4$	$16 \mapsto x^4$

(Note that although (C, \circ) is generated by x^3 , x^5 and x^7 as well as by x , mapping the generators of (G, \times_{17}) in turn to any of these generators of (C, \circ) results in the same four isomorphisms above.)

Unit B3

Permutations

Introduction

In this unit you will study groups whose elements are *permutations*. You will see that these provide us with an abundant supply of finite groups.

A *permutation* of a finite set is a function that rearranges the elements of the set. You have already met examples of permutations in this book: each two-line symbol representing a symmetry of a figure specifies a permutation of the set of location labels of the figure, since the bottom line of each two-line symbol indicates how the labels in the top line are rearranged. In this unit you will meet another notation for permutations, called *cycle form*, which is often more convenient. You will learn how to compose and find inverses of permutations written in this form, and you will see that the set of all permutations of a set of n elements forms a group under function composition.

You will go on to study some properties of permutations, and consider various subgroups of the group of all permutations of n symbols. You will also explore the idea of using one permutation to rename the symbols in another permutation, an idea that leads to the important concept of *conjugacy*.

At the end of the unit you will meet Cayley's Theorem, a result that highlights the importance of permutations in group theory. It asserts that every finite group is isomorphic to (and therefore essentially the same as) a group of permutations.

1 Permutations

In this section you will be introduced to the idea of a permutation, see how to write permutations in cycle form, and learn how to compose and invert them in this form.

1.1 Cycle form of a permutation

We begin with a definition of what we mean by a *permutation* in group theory.

Definition

A **permutation** of a finite set S is a one-to-one function from S to S .

So a permutation is a function that maps each element of a finite set to an element of the same set, in such a way that each element of the set is used exactly once as an image, as illustrated for a 5-element set in Figure 1 (there must be exactly one arrow from and to each element). Note that a function from a finite set to itself that is one-to-one must also be onto.

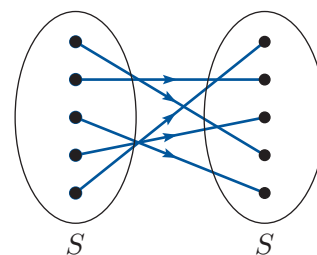


Figure 1 A permutation of a 5-element set S

We usually work with permutations of sets of the form

$$\{1, 2, 3, \dots, n\},$$

where n is a natural number. Examples of such sets include $\{1, 2, 3\}$ and $\{1, 2, 3, 4\}$. We refer to the elements of the set as the **symbols** being permuted.

A simple way of specifying a permutation is to list the symbols being permuted on one line, and the corresponding image of each symbol underneath it on a second line, enclosing the whole array in brackets. An example of a permutation of the set $\{1, 2, 3, 4, 5, 6\}$ written in this way is

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

This permutation f maps the symbols 1 to 5, 2 to 6, 3 to 1, and so on, as we see by reading downwards.

We call this notation the **two-line form** of a permutation. The format is the same as that of the *two-line symbols* that we used to represent symmetries in Units B1 and B2, and indeed those are all examples of permutations.

You may previously have seen the word ‘permutation’ used in a different but related sense, to mean an arrangement of the elements of a finite set. This is its usual meaning in the field of mathematics known as *combinatorics*. When used in this sense, a permutation does not mean a one-to-one function from a finite set to itself, but it can be thought of as the *result* of applying such a function to a list of the elements of the set, because the effect of the function is to rearrange the list. For example, the bottom row of the two-line form above is a permutation, in the combinatorial sense, of the symbols in the top row. In group theory we always use the word permutation to mean the *function* itself, as in the definition above, rather than the resulting rearrangement of the elements of the set.

There is another notation for permutations, an alternative to two-line form, which is often more convenient. Consider again the permutation f given in two-line form above. If we start at the symbol 1 and apply f repeatedly, then we get the string of symbols

$$1 \xrightarrow{f} 5 \xrightarrow{f} 4 \xrightarrow{f} 2 \xrightarrow{f} 6 \xrightarrow{f} 3 \xrightarrow{f} 1.$$

This string contains all the information needed to specify f , since it gives the image under f of each of the six symbols being permuted. It shows that f permutes the six symbols in the **cycle** shown in Figure 2.

We can use this fact to provide a more concise notation for f than the two-line form above. We write

$$f = (1\ 5\ 4\ 2\ 6\ 3),$$

with the interpretation that f maps each symbol to the one immediately to the right of it, and maps the last symbol back to the first (in this case,

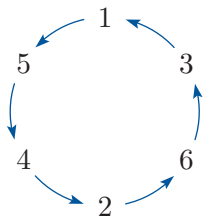


Figure 2 A cycle of six symbols

3 maps to 1). We call this the *cycle form* of f . As the cycle has no particular starting point, we can write any of the symbols first. For example, we can write

$$f = (4\ 2\ 6\ 3\ 1\ 5) \quad \text{and} \quad f = (3\ 1\ 5\ 4\ 2\ 6);$$

these convey exactly the same information and are equally good representations of f . However, when the symbols being permuted are numbers, we usually write the smallest number first in a cycle unless there is a reason to do otherwise.

Exercise B81

(a) Write down the cycle form of each of the following permutations.

$$(i) \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad (ii) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 6 & 2 & 1 & 4 \end{pmatrix}$$

(b) Write down the two-line form of each of the following permutations given in cycle form.

$$(i) (1\ 3\ 2) \quad (ii) (1\ 6\ 2\ 4\ 3\ 5)$$

(c) Can you write down a cycle corresponding to the following permutation g ? If not, why not?

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 1 & 2 & 7 & 5 \end{pmatrix}$$

Not all permutations can be written in cycle form as simply as our first example f , because not every permutation maps all the symbols in a single cycle. For example, for the permutation

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 1 & 2 & 7 & 5 \end{pmatrix}$$

in Exercise B81(c) we have

$$1 \xrightarrow{g} 4 \xrightarrow{g} 3 \xrightarrow{g} 8 \xrightarrow{g} 5 \xrightarrow{g} 1,$$

and we can write this string as the cycle $(1\ 4\ 3\ 8\ 5)$. But what about the other symbols? Starting at the symbol 2 we have

$$2 \xrightarrow{g} 6 \xrightarrow{g} 2,$$

which gives the cycle $(2\ 6)$. Also we have the symbol 7, which is mapped to itself:

$$7 \xrightarrow{g} 7.$$

We can represent this by the ‘short cycle’ (7) .

Thus g is made up of three disjoint cycles, as shown in Figure 3. We say that two or more cycles are **disjoint** if each symbol that appears in the cycles appears in only one cycle.

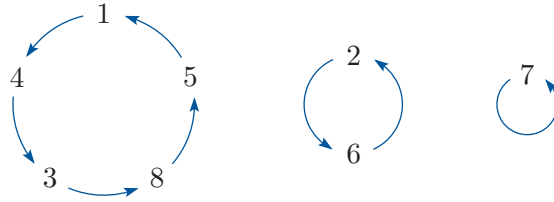


Figure 3 The cycles of the permutation g

We write the permutation g as

$$g = (1\ 4\ 3\ 8\ 5)(2\ 6)(7).$$

We call this the *cycle form* of g and say that g is the **product** of the disjoint cycles $(1\ 4\ 3\ 8\ 5)$, $(2\ 6)$ and (7) . As before, the starting point of each cycle does not matter. Also, because the three cycles are disjoint, it makes no difference if we write them in a different order. Thus we can convey the same information by writing, for example,

$$g = (6\ 2)(7)(3\ 8\ 5\ 1\ 4) \quad \text{or} \quad g = (7)(5\ 1\ 4\ 3\ 8)(2\ 6).$$

Exercise B82

Complete the following cycle forms for the permutation g above.

$$(a) \ g = (7)(8\ -\ -\ -)(6\ -) \quad (b) \ g = (5\ -\ -\ -)(2\ -)(-)$$

In general, we say that a permutation is written in **cycle form** when it is written as a product of disjoint cycles.

When the symbols being permuted are numbers, we usually write the cycle form of a permutation with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order, unless there is a reason to do otherwise. For example, we would usually write the permutation g above as

$$g = (1\ 4\ 3\ 8\ 5)(2\ 6)(7).$$

Here 1, 2 and 7 are the smallest numbers in their respective cycles, so they appear first in the cycles, and the cycles containing 1, 2 and 7, respectively, appear in that order.

The cycle form of any permutation can be found by carrying out a procedure similar to that used above for the permutation g , as outlined in the following strategy.

Strategy B7

To find the cycle form of a permutation f , do the following.

1. Choose any symbol (such as 1) and find its image under f , then find the image of its image under f , and so on, until you encounter the starting symbol again.
2. Write these symbols as a cycle.
3. Repeat the process starting with any symbol that has not yet been placed in a cycle, until all the symbols have been placed in cycles.



When you use Strategy B7, it does not matter which symbol you choose to start each new cycle, as long as it is one that you have not yet placed in a cycle. However, if the symbols are numbers, and you always choose the smallest number not yet placed in a cycle, then you will automatically obtain the cycle form of the permutation written in the usual way described above (that is, with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order). This is demonstrated in the worked exercise below.

Worked Exercise B32



Find the cycle form of the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 7 & 5 & 3 & 4 \end{pmatrix}.$$



Solution

 Start the first cycle with the smallest symbol, 1. This gives $1 \rightarrow 6 \rightarrow 3 \rightarrow 1$. 

$$f = (1\ 6\ 3)\dots$$

 Start the next cycle with the smallest symbol not yet placed in a cycle, which is 2. This gives $2 \rightarrow 2$. 

$$f = (1\ 6\ 3)(2)\dots$$

 Continue in the same way to obtain the remaining cycles. This gives $4 \rightarrow 7 \rightarrow 4$ and $5 \rightarrow 5$. 

$$f = (1\ 6\ 3)(2)(4\ 7)(5).$$

 All the symbols have now been placed in cycles, so the cycle form is complete. 

You may have wondered how we can be sure that we will eventually encounter the starting symbol again in step 1 of Strategy B7. To see why this is, first note that because there are only finitely many symbols, at some point we must encounter again some symbol that we have encountered before. Let x be the first symbol that we encounter twice. If x were not the symbol that we started with, then x would be the image under f of two different symbols (the symbols encountered immediately before the two occurrences of x), and this cannot happen because f is one-to-one.

Exercise B83

- (a) Convert the following permutations from two-line form to cycle form.
- (i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 1 & 5 & 3 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 9 & 1 & 3 & 8 & 2 & 6 & 4 \end{pmatrix}$
- (b) Convert the following permutations from cycle form to two-line form.
- (i) $(1\ 6)(2\ 3\ 7\ 5)(4)$ (ii) $(1\ 6\ 4\ 2)(3\ 5\ 8)(7)$

Since Strategy B7 can be applied to any permutation, and since it must always give the same cycles for any particular permutation, we have the following result.

Theorem B51

Every permutation can be written in cycle form. The cycle form of a permutation is unique, apart from the choice of starting symbol in each cycle and the order in which the cycles are written.

When a cycle of a permutation consists of a single symbol, the permutation maps that symbol to itself. We say that the symbol is **fixed** by the permutation. For example, the permutation

$$f = (1\ 6\ 3)(2)(4\ 7)(5)$$

fixes both the symbols 2 and 5.

Usually, we omit cycles containing a single symbol from the cycle form of a permutation. For example, if it is clear from the context that the permutation f above permutes the symbols of the set $\{1, 2, 3, 4, 5, 6, 7\}$, then we write

$$f = (1\ 6\ 3)(4\ 7),$$

and it is understood that the missing symbols 2 and 5 are fixed by f .

Exercise B84

Convert the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 4 & 8 & 3 & 6 & 1 & 5 \end{pmatrix}$$

from two-line form to cycle form, omitting any cycles that contain a single symbol from the final cycle form.

The **identity permutation** of a set S is the permutation of S that fixes every symbol. For example, the identity permutation of the set $S = \{1, 2, 3, 4, 5, 6, 7\}$ has the two-line form

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

The cycle form of this permutation can be written as

$$(1)(2)(3)(4)(5)(6)(7).$$

Unfortunately, if we omit the cycles containing a single symbol from this cycle form, then there is nothing left! For this reason, when we work with cycle forms, we usually denote the identity permutation simply by e .

The two conventions described above are summarised in the box below.

Cycle form conventions

- When it is clear from the context which set of symbols is being permuted, we omit fixed symbols from the cycle form of a permutation.
- When working with permutations in cycle form, we denote the identity permutation by e .

Exercise B85

Write down the two-line form of each of the following permutations of $\{1, 2, 3, 4, 5\}$.

- (a) $(1\ 4)(2\ 5)$ (b) $(1\ 2)$ (c) $(1\ 5\ 4)$ (d) e

The notations that we call the two-line form and the cycle form of a permutation were both introduced by the French mathematician Augustin-Louis Cauchy (1789–1857), in two major papers in which he launched the subject of permutations as an independent area of study. The two-line form appeared in the paper of 1815, and the cycle form appeared nearly 30 years later in the paper of 1844.



Augustin-Louis Cauchy

1.2 Composing permutations

A composite of two permutations is a permutation, because if f and g are functions that map a set S to itself, then so does $g \circ f$; and if f and g are both one-to-one, then so is $g \circ f$.

In Unit B1 *Symmetry* you saw how to compose two symmetries written as two-line symbols; we can use the same method to compose any two permutations written in two-line form. However, when we want to compose two permutations that are written in cycle form, we can do so without having to first convert them to two-line form, as demonstrated in the next worked exercise.

Worked Exercise B33

Let $f = (1\ 4\ 3)(2\ 6)$ and $g = (1\ 4\ 6\ 2\ 5)$ be permutations of $\{1, 2, 3, 4, 5, 6\}$. Find the cycle form of $g \circ f$.

Solution

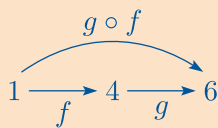
Write down the cycle forms of f and g , in the right order.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6)$$

Remember that, as f and g are functions, the composite permutation $g \circ f$ means ‘first f , then g ’. Start the first cycle of $g \circ f$ with the smallest symbol, 1.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1 \dots$$

Find the image of 1 under $g \circ f$. We see that f (the first permutation) maps 1 to 4, then g maps 4 to 6:



So $g \circ f$ maps 1 to 6.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6 \dots$$

To continue the cycle, find the image of 6. We see that f maps 6 to 2, then g maps 2 to 5, so $g \circ f$ maps 6 to 5.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5 \dots$$

Continue in the same way. Next we see that f fixes 5, then g maps 5 to 1, so $g \circ f$ maps 5 to 1. Since 1 is the start of the cycle, the cycle is complete.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5) \dots$$

Now start a new cycle with the smallest symbol not yet placed in a cycle, which is 2.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2\ \dots$$

We see that f maps 2 to 6, then g maps 6 to 2, so $g \circ f$ fixes 2. So this cycle is complete.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2)$$

Start a new cycle with the smallest symbol not yet placed in a cycle, which is 3.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2)(3\ \dots$$

To continue the cycle, find the image of 3. We see that f maps 3 to 1, then g maps 1 to 4, so $g \circ f$ maps 3 to 4.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2)(3\ 4\ \dots$$

Next, we see that f maps 4 to 3, then g fixes 3, so $g \circ f$ maps 4 to 3. Since 3 is the start of the cycle, the cycle is complete.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2)(3\ 4)$$

All six symbols have now been placed in cycles, so the cycle form is complete.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2)(3\ 4) = (1\ 6\ 5)(3\ 4).$$

Note that if

$$f = (1\ 4\ 3)(2\ 6) \quad \text{and} \quad g = (1\ 4\ 6\ 2\ 5),$$

as in the worked exercise above, then although it is true that

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6),$$

the expression on the right here is *not a cycle form*, because the cycles are *not disjoint* – some symbols are repeated. The correct cycle form of $g \circ f$ is as found in the worked exercise.

The strategy below summaries the method used in Worked Exercise B33.

Strategy B8

To find the composite $g \circ f$ of two permutations written in cycle form, do the following.

1. Start with the smallest symbol, 1 say. Find the symbol that is the image of 1 under f , then find the image of that symbol under g , and write the result, x say, next to 1 in a cycle:

$$(1 \ x \ \dots$$

2. Starting with the symbol x , repeat the process to obtain the next symbol in the cycle.
3. Continue repeating the process until the next symbol found is the original symbol 1. This completes the cycle.
4. Starting with the smallest symbol not yet placed in a cycle, repeat steps 1 to 3 until every symbol has been placed in a cycle.
5. Usually, rewrite the cycle form omitting the cycles containing a single symbol, if there are any.

When you use Strategy B8, it is not strictly necessary to start each new cycle with the *smallest* symbol not yet placed in a cycle – any symbol not yet placed in a cycle will do. However, if you always choose the smallest symbol, then the cycle form you obtain will automatically be written in the conventional way (that is, with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order).

Exercise B86

Let $f = (1 \ 4 \ 3)(2 \ 6)$ and $g = (1 \ 4 \ 6 \ 2 \ 5)$ be permutations of $\{1, 2, 3, 4, 5, 6\}$, as in Worked Exercise B33. Use Strategy B8 to determine each of the following permutations in cycle form.

(a) $f \circ g$ (b) $f \circ f$ (c) $g \circ g$

Worked Exercise B33 and Exercise B86(a) illustrate the fact that the order in which two permutations are composed is important: for the permutations f and g here,

$$g \circ f \neq f \circ g.$$

In general, if f and g are permutations, then the composite permutations $g \circ f$ and $f \circ g$ are usually not equal. That is, composition of permutations is not *commutative* (as is true for functions in general).

Exercise B87

Let $f = (1\ 3\ 2\ 4\ 6)$ and $g = (1\ 4)(3\ 5)$ be permutations of $\{1, 2, 3, 4, 5, 6\}$. Determine each of the following permutations in cycle form.

- (a) $g \circ f$ (b) $f \circ g$ (c) $f \circ f$ (d) $g \circ g$

Sometimes we need to find a composite of three or more permutations. One way to do this is to deal with the permutations two at a time, using Strategy B8. For example, if you want to find a composite $h \circ g \circ f$, then you can first use Strategy B8 to find $g \circ f$, and then use it again to find $h \circ (g \circ f)$.

However, it is more efficient to deal with all the permutations at the same time, by adapting Strategy B8. This is demonstrated in the next worked exercise.

Worked Exercise B34

Determine the cycle form of the following permutation of the set $\{1, 2, 3, 4, 5, 6\}$:

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6).$$

Solution

Start the first cycle of the composite permutation with the smallest symbol, 1.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1 \dots$$

Find the image of 1 under the composite permutation. Remember that the permutations are carried out in order *from right to left*. The first permutation maps 1 to 2, the second maps 2 to 4 and the third maps 4 to 6:



So the composite permutation maps 1 to 6.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6 \dots$$

To continue the cycle, find the image of 6. The first permutation maps 6 to 4, the second maps 4 to 1 and the third maps 1 to 4, so the composite permutation maps 6 to 4.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4 \dots$$

Next, find the image of 4. The first permutation maps 4 to 6, the second maps 6 to itself and the third maps 6 to 1, so the composite permutation maps 4 to 1. Since 1 is the start of the cycle, the cycle is complete.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4) \dots$$

Now start a new cycle with the smallest symbol not yet placed in a cycle, which is 2.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2 \dots$$

Find the image of 2. The first permutation maps 2 to 1, the second maps 1 to 5 and the third maps 5 to 3, so the composite permutation maps 2 to 3.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3 \dots$$

Continue the cycle by finding the image of 3. The first permutation maps 3 to 5, the second maps 5 to 3 and the third maps 3 to 5, so the composite permutation maps 3 to 5.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3\ 5 \dots$$

Now find the image of 5. The first permutation maps 5 to 3, the second maps 3 to 2 and the third fixes 2, so the composite permutation maps 5 to 2. Since 2 is the start of the cycle, the cycle is complete.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3\ 5)$$

All six symbols have now been placed in cycles, so the cycle form is complete.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3\ 5)$$

Exercise B88

Determine the cycle form of each of the following permutations of $\{1, 2, 3, 4, 5, 6, 7\}$.

(a) $(1\ 3)(2\ 4)(5\ 7\ 6) \circ (1\ 7\ 6)(2\ 3) \circ (1\ 7\ 4\ 6)$

(b) $(1\ 7\ 3\ 4\ 6) \circ (1\ 2) \circ (3\ 7) \circ (5\ 3)$

It is useful to note that any permutation is equal to the composite of its disjoint cycles. For example, consider the following permutation of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, written in cycle form:

$$f = (1\ 3)(2\ 4\ 9\ 6)(5\ 7\ 8).$$

Each of the three disjoint cycles in this cycle form is a permutation in its own right; for example, $(1\ 3)$ is the permutation that interchanges the symbols 1 and 3 and leaves all the other symbols fixed. Furthermore, the overall effect of f is the same as the effect of first performing the permutation $(5\ 7\ 8)$, then $(2\ 4\ 9\ 6)$ and then $(1\ 3)$, so f is the composite of these three permutations. That is,

$$f = (1\ 3) \circ (2\ 4\ 9\ 6) \circ (5\ 7\ 8).$$

In fact, since these three permutations are disjoint cycles, f is their composite *in any order*. We will use the fact that any permutation is equal to the composite of its disjoint cycles later in the unit.

In many texts on group theory, a composite of permutations is called a *product* of permutations, and, accordingly, the operation of forming such a composite is denoted by juxtaposition rather than by the symbol \circ . (To **juxtapose** objects is to place them next to each other.) For example, the composite $(1\ 2\ 3)(4\ 5) \circ (2\ 4)$ of the two permutations $(2\ 4)$ and $(1\ 2\ 3)(4\ 5)$ would be denoted simply by $(1\ 2\ 3)(4\ 5)(2\ 4)$.

In this module, however, we reserve the word ‘product’ for composites of disjoint cycles, and we usually retain the use of the symbol \circ for the operation of composition of permutations.

1.3 Finding the inverse of a permutation

Since every permutation f is a one-to-one function, it has an inverse function f^{-1} , which we call the **inverse permutation** of f .

You have seen that every permutation f is made up of disjoint cycles. Since the inverse f^{-1} of f undoes what f does – that is, if f maps x to y , then f^{-1} maps y to x – it follows that f^{-1} is obtained from f by reversing the direction of the disjoint cycles of f .

For example, consider the permutation f whose disjoint cycles are shown in Figure 4(a). The disjoint cycles of its inverse f^{-1} are shown in Figure 4(b).

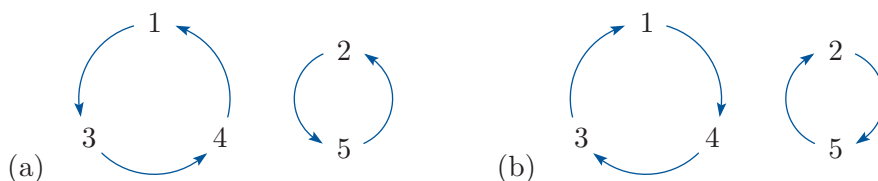


Figure 4 (a) The cycles of a particular permutation f (b) The cycles of f^{-1}

So we have the following strategy for finding the inverse of a permutation written in cycle form. It is illustrated in the worked exercise below for the permutation f in Figure 4.

Strategy B9

To find the inverse of a permutation written in cycle form, do the following.

1. Reverse the order of the symbols in each cycle.
2. Then, usually, rewrite each cycle so that the smallest symbol is first.

Worked Exercise B35



Determine the inverse of the following permutation of $\{1, 2, 3, 4, 5\}$:

$$f = (1\ 3\ 4)(2\ 5).$$

Solution

 Reverse the order of the symbols in each cycle. 

$$f^{-1} = (4\ 3\ 1)(5\ 2)$$

 Rewrite each cycle with the smallest symbol first. 

$$= (1\ 4\ 3)(2\ 5)$$

You can confirm that the inverse permutation found in Worked Exercise B35 is correct by checking that $f \circ f^{-1} = e = f^{-1} \circ f$, that is,

$$(1\ 3\ 4)(2\ 5) \circ (1\ 4\ 3)(2\ 5) = e = (1\ 4\ 3)(2\ 5) \circ (1\ 3\ 4)(2\ 5).$$

Exercise B89

Write down the inverse of each of the following permutations of $\{1, 2, 3, 4, 5, 6, 7, 8\}$.

- (a) $(1\ 6\ 4\ 2\ 5\ 8\ 3\ 7)$ (b) $(1\ 5\ 4\ 7)(2\ 6\ 8)$ (c) $(1\ 8)(2\ 7)(3\ 5)$

Exercise B90

Let f and g be the following permutations of $\{1, 2, 3, 4, 5, 6\}$:

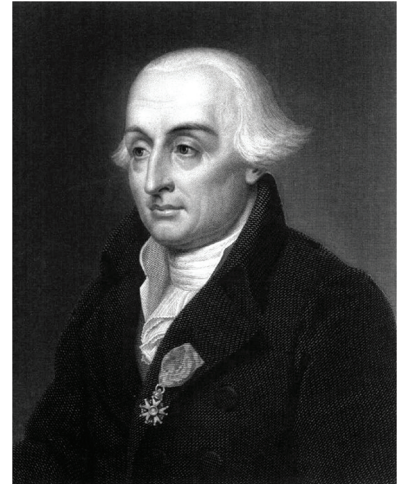
$$f = (1\ 2\ 6\ 4\ 5), \quad g = (1\ 3\ 6)(2\ 5\ 4).$$

- (a) Write down the following permutations in cycle form.

(i) $g \circ f$ (ii) f^{-1} (iii) g^{-1} (iv) $(g \circ f)^{-1}$

- (b) Verify that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Permutations have been an object of study for many centuries. For example, they appear in India as early as 1150 in the work of Bhāskara II (1114–1185). However, from the point of view of group theory, the starting point for their study is a paper by Joseph-Louis Lagrange (1736–1813) of 1770/71 on the theory of algebraic equations.



Joseph-Louis Lagrange

2 Permutation groups

We now go on to look at some groups whose elements are permutations, and some properties of the permutations in these groups.

2.1 The symmetric group S_n

We denote the set of all permutations of the set $\{1, 2, 3, \dots, n\}$ by S_n . The set S_n forms a group under function composition, as stated and proved below.

Theorem B52

The set S_n of all permutations of the set $\{1, 2, 3, \dots, n\}$ is a group under function composition.

Proof We check that the four group axioms hold. (The group axioms were given in Subsection 3.1 of Unit B1.)

Let $S = \{1, 2, 3, \dots, n\}$.

G1 Closure

We have seen that the composite $g \circ f$ of any two permutations f and g of S is itself a permutation of S . That is, for all $f, g \in S_n$, we have $g \circ f \in S_n$.

G2 Associativity

Function composition is an associative binary operation.

G3 Identity

The identity permutation e , which fixes every symbol of S , is an identity element in S_n .

G4 Inverses

We have seen that each permutation f of the set S has an inverse permutation f^{-1} , which is also a permutation of S . (The permutations f and f^{-1} satisfy the equation $f \circ f^{-1} = e = f^{-1} \circ f$ by the definition of an inverse function: see the discussion at the end of Section 3.4 in Unit A1 *Sets, functions and vectors*.) That is, each permutation $f \in S_n$ has an inverse $f^{-1} \in S_n$.

Hence S_n is a group. ■

In Unit B2 you met the convention that if the binary operation of a group (G, \circ) is clear from the context, then we often refer to the group simply as the group G , rather than the group (G, \circ) . We use this convention for the group (S_n, \circ) : we usually refer to it simply as the group S_n , with the understanding that the binary operation is function composition.

Definition

The group S_n of all permutations of the set $\{1, 2, 3, \dots, n\}$ is called the **symmetric group of degree n** .

Although the symmetric group S_n is defined to be the group of all permutations of the set $\{1, 2, 3, \dots, n\}$, notice that the actual symbols being permuted do not matter in the proof of Theorem B52 above, so the proof shows that the set of permutations of *any* set of n symbols forms a group under function composition. Sometimes it is useful to take the set of n symbols being permuted to be a set other than the usual set $\{1, 2, 3, \dots, n\}$, as you will see later.



William Burnside

The term *symmetric group* first appeared in English in 1897 in *Theory of Groups of Finite Order*, the classic work of William Burnside (1852–1927) and the first treatise on group theory in English. Burnside, who began his career at the University of Cambridge, was professor of mathematics at the Royal Naval College at Greenwich from 1885 until 1919. He was one of the leading group theorists of his generation.

Be careful not to confuse a *symmetric* group with a *symmetry* group: a symmetry group is a group of symmetries of a figure.

Also, be careful not to confuse the *degree* and the *order* of a symmetric group. Its degree is the number of symbols that its elements permute, whereas, just as for any group, its **order** is the number of elements that it has. In the next exercise you are asked to find the orders of the symmetric groups S_3 and S_4 .

Exercise B91

- Write down all the elements of the group S_3 in two-line form and also in cycle form. What is the order of the group S_3 ?
- What is the order of the group S_4 ?

Hint: Do not attempt to write down all the elements of S_4 . Instead, try to count how many different ways there are to complete the bottom row of the two-line form of a permutation of the set $\{1, 2, 3, 4\}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}.$$

The solution to Exercise B91 can be generalised to prove the theorem below. Remember that for any positive integer n , we write

$$n! = n \times (n - 1) \times \cdots \times 2 \times 1.$$

This number is called the **factorial** of n . The notation $n!$ is read as ‘ n factorial’ or ‘factorial n ’.

Theorem B53

The symmetric group S_n has order $n!$.

Proof We count how many different ways there are to complete the bottom row of the two-line form of a permutation of the set $\{1, 2, 3, \dots, n\}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \end{pmatrix}.$$

There are n choices for the symbol to be placed in the first position in the bottom row.

Once we have chosen this symbol, there are only $n - 1$ symbols still to be placed, so there are $n - 1$ choices for the symbol to be placed in the second position.

Once we have chosen the first two symbols, there are only $n - 2$ symbols still to be placed, so there are $n - 2$ choices for the symbol to be placed in the third position.

We continue in this way, until, finally, there are 2 choices for the symbol to be placed in the $(n - 1)$ th position, and then just 1 choice for the symbol to be placed in the n th position.

The total number of ways to fill in the bottom row is therefore

$$n \times (n - 1) \times (n - 2) \times \cdots \times 2 \times 1 = n!.$$

That is, the group S_n has order $n!$. ■

The order of the group S_n grows very quickly as n increases. For example,

$$\begin{aligned} |S_3| &= 3! = 6, \\ |S_4| &= 4! = 24, \\ |S_5| &= 5! = 120, \\ |S_6| &= 6! = 720, \\ |S_7| &= 7! = 5040, \\ |S_8| &= 8! = 40\,320. \end{aligned}$$

(Remember that the order of a group G is denoted by $|G|$.)

Even for quite small values of n , the group S_n has many subgroups.

Definition

A **permutation group** (or **group of permutations**) is a subgroup of the group S_n , for some positive integer n .

For example, the subset

$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

of the group S_4 is a permutation group, since it is a subgroup of S_4 , as you will see in Subsection 2.4.

We will find more subgroups of symmetric groups in the next two subsections, and we will find all the subgroups of the particular symmetric group S_4 in Section 5.

2.2 Cycle structure

In this subsection we look at the different possible structures of the cycle form of a permutation.

The simplest type of structure is a single cycle, as defined below.

Definitions

A permutation whose cycle form consists of a single cycle permuting r symbols (with all other symbols fixed) is called an **r -cycle** or a **cycle of length r** .

A 2-cycle is also called a **transposition**.

For example, in S_5 ,

the permutation $(1\ 5\ 2\ 4\ 3)$ is a 5-cycle

the permutation $(1\ 2\ 5\ 3)$ is a 4-cycle

the permutation $(2\ 4\ 5)$ is a 3-cycle

the permutations $(1\ 5)$ and $(2\ 3)$ are transpositions.

The following two permutations in S_5 have a cycle form that consists of more than one cycle:

the permutation $(1\ 2\ 5)(3\ 4)$ consists of a 2-cycle and a 3-cycle

the permutation $(1\ 3)(2\ 4\ 5)$ also consists of a 2-cycle and a 3-cycle.

We say that these two permutations have the *same cycle structure* in S_5 .

Definition

Two permutations in S_n have the **same cycle structure** if their cycle forms contain the same number of disjoint r -cycles for each natural number r .

For example, in S_8 , the permutations

$$(1\ 2\ 4)(3\ 8)(5\ 6) \quad \text{and} \quad (1\ 7)(2\ 8\ 3)(4\ 5)$$

have the same cycle structure, since each consists of a 3-cycle, two 2-cycles and a 1-cycle (the 1-cycle is for the fixed symbol that does not appear in the cycle form). On the other hand, the permutations

$$(2\ 6\ 3)(4\ 8) \quad \text{and} \quad (1\ 8)(2\ 3)(4\ 6\ 7)$$

in S_8 have different cycle structures, since, for example, the first permutation has just one 2-cycle whereas the second has two.

The concept of cycle structure is useful when we want to determine all the permutations in S_n in cycle form for a particular value of n . We can start by working out which cycle structures are possible.

Worked Exercise B36

Write down all the possible cycle structures in S_3 , and list all the permutations in S_3 with each cycle structure.

Solution

There are three possible cycle structures in S_3 . These are given in the table below, together with the corresponding elements of S_3 .

Cycle structure	Elements of S_3	Description
e	e	identity
$(- \ -)$	$(1\ 2), (1\ 3), (2\ 3)$	transpositions
$(- \ - \ -)$	$(1\ 2\ 3), (1\ 3\ 2)$	3-cycles

In Worked Exercise B36 we could have written the cycle structure of the identity permutation e as $(-)(-)(-)$, but it is more convenient just to write e .

Exercise B92

Write down all the possible cycle structures in S_4 , and give one permutation with each cycle structure.

Exercise B93

Find as many cycle structures as you can in S_5 , and write down one permutation with each cycle structure you find.

2.3 Order of a permutation

In Unit B2 you saw that the **order** of an element x of a group (G, \circ) is the smallest positive integer n such that $x^n = e$. In this subsection we will look at how we can determine the order of a permutation in S_n .

Let us start by investigating the order of a permutation that consists of a single cycle. Consider, for example, the following 5-cycle in S_6 :

$$f = (1\ 3\ 2\ 4\ 6).$$

We can find the order of f by evaluating f^2, f^3, \dots , until we reach the identity permutation e . (Remember that f^2 denotes $f \circ f$, and f^3 denotes $f \circ f \circ f$, and so on.) These powers of f can be found by using the usual method for composing permutations, but there is a quicker way: they can be read from the cycle form of f .

For example, the permutation f^2 is obtained by applying f twice to each symbol, which amounts to mapping each symbol to the symbol two places around the cycle, as shown in Figure 5(a).

Therefore

$$f^2 = (1\ 2\ 6\ 3\ 4).$$

(The symbol 5 is fixed by f and by any power of f .)

Similarly, f^3 maps each symbol to the symbol three places around the cycle, as shown in Figure 5(b).

Therefore

$$f^3 = (1\ 4\ 3\ 6\ 2).$$

Applying f four times maps each symbol to the symbol four places around the cycle (or, equivalently, one place backwards), as shown in Figure 5(c).

Therefore

$$f^4 = (1\ 6\ 4\ 2\ 3).$$

Applying f five times maps each symbol to the symbol five places around the cycle; that is, f^5 maps each symbol to itself, so

$$f^5 = e.$$

Hence f has order 5.

In general, for any cycle in any symmetric group S_n , we have the following result.

Theorem B54

An r -cycle has order r .

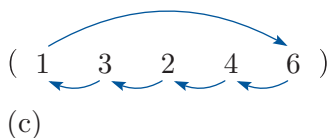
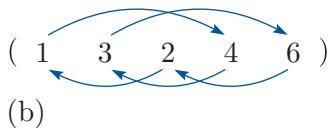
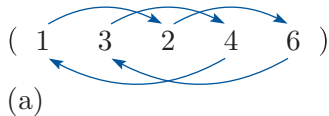


Figure 5 Mapping each symbol round a cycle (a) by two places (b) by three places (c) by four places

Proof Consider an r -cycle $f = (a_1 a_2 \dots a_r)$. To prove that f has order r , we need to show that $f^r = e$ and also that $f^k \neq e$ for any positive integer $k < r$.

The permutation f^r (r applications of f) takes each symbol r places around the cycle; that is, back to itself. Thus f^r fixes each symbol, so $f^r = e$.

Also, for each positive integer $k < r$, the k th power of f takes each symbol k places around the cycle to a *different* symbol. Thus $f^k \neq e$.

It follows that the order of f is r . ■

Exercise B94

Verify Theorem B54 when f is the 6-cycle $(1\ 6\ 3\ 7\ 5\ 2)$ in S_7 , by finding powers f^k of f for $k = 1, 2, 3, \dots$ until you reach the identity permutation.

Now let us look at the question of how to determine the order of a permutation that consists of more than one disjoint cycle. Consider, for example, the following permutation f in S_9 :

$$f = (1\ 2)(3\ 4\ 5\ 6)(7\ 8\ 9).$$

Since, for any positive integer k , the k th power f^k of f moves each symbol k places around the cycle of f in which it lies, we can deduce which symbols are fixed by the various powers of f , as follows:

1 and 2 are fixed by the 2nd, 4th, 6th, 8th, 10th, 12th, ... powers of f

3, 4, 5 and 6 are fixed by the 4th, 8th, 12th, ... powers of f

7, 8 and 9 are fixed by the 3rd, 6th, 9th, 12th, ... powers of f .

The smallest positive power of f that fixes all nine symbols is the 12th power, so f has order 12.

The answer 12 here is the *least common multiple* of the lengths 2, 3 and 4 of the cycles of f . Remember that the **least common multiple** of a set of non-zero integers is the smallest positive integer that is divisible by each number in the set.

The order of any permutation can be worked out in a similar way. So we have the following general result.

Theorem B55



The order of a permutation is the least common multiple of the lengths of its cycles.

Worked Exercise B37

Write down the order of the permutation

$$(1\ 4\ 8\ 5\ 6\ 9)(2\ 3\ 7).$$

Solution

 The cycle lengths are 6 and 3, and the least common multiple of 6 and 3 is 6. 

The permutation has order 6.

Exercise B95

Write down the order of each of the following permutations.

(a) $(3\ 5\ 4\ 9)(1\ 6)(2\ 7)$ (b) $(1\ 5\ 9)(2\ 8\ 3\ 7\ 4)$

(c) $(1\ 2)(3\ 9)(4\ 8)(5\ 6\ 7)$ (d) $(1\ 5\ 9)(2\ 4\ 6)$

As you saw in Unit B2, an element f of order n in a group G generates a cyclic subgroup $\langle f \rangle$ of order n , given by

$$\langle f \rangle = \{e, f, f^2, \dots, f^{n-1}\}.$$

Worked Exercise B38

Find the elements of the cyclic subgroup $\langle (1\ 2\ 3) \rangle$ of S_4 .

Solution

The permutation $(1\ 2\ 3)$ has order 3, so

$$\begin{aligned} \langle (1\ 2\ 3) \rangle &= \{e, (1\ 2\ 3), (1\ 2\ 3)^2\} \\ &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}. \end{aligned}$$

Exercise B96

Find the elements of each of the following cyclic subgroups of S_5 .

(a) $\langle (1\ 5\ 2\ 3) \rangle$ (b) $\langle (1\ 4\ 2)(3\ 5) \rangle$

Exercise B97

Show that the set $S = \{e, (1\ 5\ 6), (1\ 6\ 5)\}$ is a subgroup of S_6 .

2.4 Representing symmetries as permutations

In Unit B1 you saw that the symmetries of any figure F in \mathbb{R}^2 or \mathbb{R}^3 form a group under function composition, called the *symmetry group* of F and denoted by $S(F)$. You saw that if F is a polygon or polyhedron then by labelling its vertex locations we can represent its symmetries as two-line symbols.

For example, consider the square with its vertex locations labelled with the symbols 1, 2, 3 and 4 in the usual way, as shown in Figure 6. With this labelling we can represent the symmetries a and s , for instance, of the square by

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \text{and} \quad s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Since the two-line symbols that represent the symmetries of the square are permutations of the set $\{1, 2, 3, 4\}$ in two-line form, they are elements of the symmetric group S_4 . So we can also write them in cycle form. For instance, for the two symmetries above we have

$$a = (1\ 2\ 3\ 4) \quad \text{and} \quad s = (2\ 4).$$

Cycle form is usually more convenient than two-line symbols for representing the symmetries of a figure. For example, the cycle forms above for the symmetries a and s of the square make it obvious that a maps the four vertices of the square round in a cycle, and that s interchanges the vertices at locations 2 and 4 and fixes the vertices at locations 1 and 3. So we will use cycle form rather than two-line symbols to represent elements of symmetry groups from now on.

When we want to write down the cycle form of a symmetry of a figure we can do so directly, rather than first writing it as a two-line symbol and then converting it. For example, we can see from Figure 6 that the symmetry r of the square interchanges the vertices at locations 1 and 4 and also interchanges the vertices at locations 2 and 3, so

$$r = (1\ 4)(2\ 3).$$

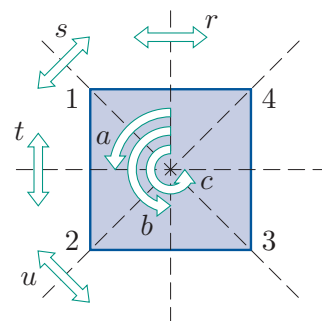


Figure 6 $S(\square)$

All the symmetries of the square are listed in cycle form in Table 1, along with their orders. The orders of these symmetries were found in Unit B1, but notice that we can also find them directly from the cycle forms using Theorem B55. For example, the symmetry r consists of two 2-cycles, so its order is the least common multiple of 2 and 2, which is 2.

Table 1 The symmetries in $S(\square)$ in cycle form

	Symmetry	Order
Rotations	e	1
	$a = (1\ 2\ 3\ 4)$	4
	$b = (1\ 3)(2\ 4)$	2
	$c = (1\ 4\ 3\ 2)$	4
Reflections	$r = (1\ 4)(2\ 3)$	2
	$s = (2\ 4)$	2
	$t = (1\ 2)(3\ 4)$	2
	$u = (1\ 3)$	2

As you saw in Unit B1 (with two-line symbols), we can compose symmetries of the square by composing the permutations that represent them. Since the symmetries of the square *form a group*, it follows that the eight permutations in Table 1 form a subgroup of the group S_4 . So $S(\square)$ can be regarded as a subgroup of S_4 .

Similarly, if we label the vertex locations of the equilateral triangle with the symbols 1, 2 and 3, then the permutations of these symbols that represent the symmetries of the triangle form a subgroup of the group S_3 . So $S(\triangle)$ can be regarded as a subgroup of S_3 . (In fact, since also $S(\triangle)$ and S_3 have the same order, $S(\triangle)$ can be regarded as being equal to S_3 .)

The same is true in general: if a figure has n vertices and we label the locations of these vertices with the symbols $1, 2, \dots, n$, then the permutations of these symbols that represent the symmetries of the figure form a subgroup of the group S_n .

Exercise B98

Write down in cycle form all the symmetries of the equilateral triangle, when the triangle is labelled in the usual way, as shown in Figure 7. State the order of each symmetry.

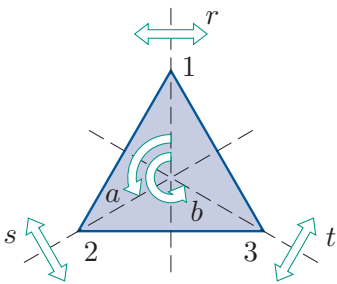


Figure 7 $S(\triangle)$

Exercise B99

Write down in cycle form all the symmetries of the rectangle, when the rectangle is labelled in the usual way, as shown in Figure 8. State the order of each symmetry.

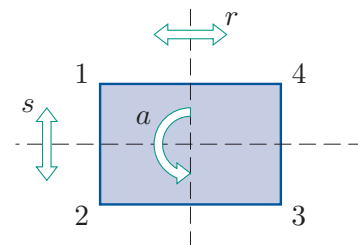
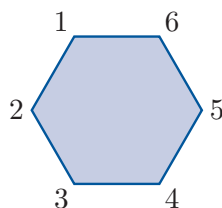


Figure 8 $S(\square)$

Exercise B100

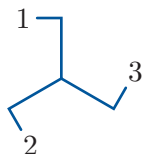
Write down in cycle form all the symmetries of the labelled regular hexagon shown below, and state the order of each symmetry. You do not need to use letters to denote the symmetries.



We can often use permutations to represent the symmetries of a plane figure even if it is not a polygon, as illustrated by the following exercise.

Exercise B101

Write down the permutations in S_3 that represent the symmetries of the following labelled figure.

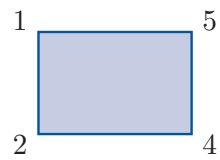


Now consider Exercise B99 again, in which the vertex locations of the rectangle were labelled with the symbols 1, 2, 3, 4 in the usual way, and the symmetries of the rectangle were represented as permutations of these symbols. These permutations form a subgroup of the symmetric group S_4 . Suppose now that we introduce a fifth symbol, 5, but do not use it to label anything. Then we can regard the permutations representing the symmetries of the rectangle as permutations of the symbols 1, 2, 3, 4, 5, with all of the permutations fixing the symbol 5. So the permutations then form a subgroup of the symmetric group S_5 .

In the same way, we can choose any four symbols from the five symbols 1, 2, 3, 4, 5, use them to label the vertex locations of the rectangle, and hence obtain a subgroup of the symmetric group S_5 . Each permutation in this subgroup fixes the symbol not used as a label. This is illustrated in the next exercise.

Exercise B102

Find a subgroup of the symmetric group S_5 by writing down in cycle form all the symmetries of the rectangle when it is labelled as shown below.



We can use the same idea to obtain a subgroup of the symmetric group S_6 . We label the vertices of the rectangle with four symbols from the set $\{1, 2, 3, 4, 5, 6\}$ and regard the other two symbols as fixed.

In general, if we label the vertex locations of a figure with some or all of the symbols from the set $\{1, 2, \dots, n\}$, then the permutations of these symbols that represent the symmetries of the figure form a subgroup of the symmetric group S_n . Any symbols in $\{1, 2, \dots, n\}$ that are not used to label the figure are taken to be fixed. Later in the unit we will use this idea to find some of the subgroups of the symmetric group S_4 .

So far we have represented the symmetries of a figure as permutations by labelling the *vertex* locations of the figure. However, we can represent the symmetries of a figure as permutations in other ways, by labelling the locations of other features of the figure, such as its edges.

Exercise B103

The edge locations of a rectangle are labelled 1, 2, 3 and 4 as shown below. Write down, in cycle form, the four elements of the group $S(\square)$ when they are expressed as permutations of these four symbols. (The non-identity elements of $S(\square)$ are shown in Figure 9.)

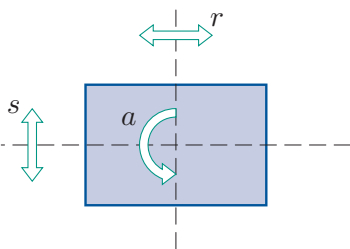
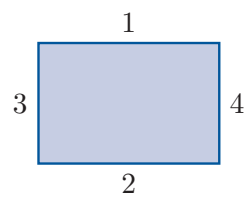


Figure 9 $S(\square)$

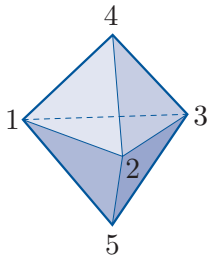
We can represent the symmetries of a figure in \mathbb{R}^3 by permutations in cycle form in the same way as the symmetries of a plane figure. As with plane figures, the symmetries of a figure in \mathbb{R}^3 form a group, so when they are represented by permutations they form a subgroup of a symmetric group.

The next worked exercise involves the symmetries of the **double tetrahedron**, which is the solid formed by sticking together two regular tetrahedrons of the same size, as illustrated in the worked exercise.

Remember from Unit B1 that the **direct** symmetries of a figure in \mathbb{R}^3 are those that can be demonstrated physically with a model of the figure; for a bounded figure these are the rotations. The symmetries that cannot be demonstrated physically with a model are the **indirect** symmetries. By Theorem B22 in Unit B1, if a figure in \mathbb{R}^3 has a finite number of symmetries, then either all the symmetries are direct, or half of the symmetries are direct and half are indirect. If there are indirect symmetries, then they can all be found by composing any fixed indirect symmetry with all of the direct symmetries.

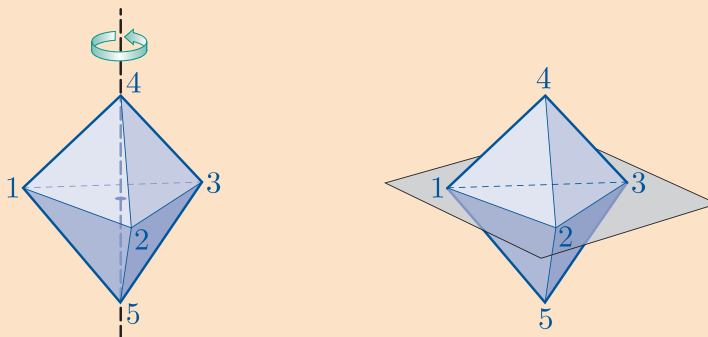
Worked Exercise B39

Write down the permutations in S_5 that represent the symmetries of the labelled double tetrahedron illustrated below.



Solution

First we determine how many symmetries the double tetrahedron has. There are six ways to pick it up and replace it to occupy its original space: we can rotate it about the vertical line through the vertices at locations 4 and 5, as shown on the left below, through angles of 0 , $2\pi/3$ or $4\pi/3$, and we can turn it upside down and then do the same three rotations. Thus the double tetrahedron has six direct symmetries. It also has at least one indirect symmetry, such as reflection in the plane through the vertices at locations 1, 2 and 3, as shown on the right below. Since any figure with at least one indirect symmetry has the same number of indirect symmetries as direct symmetries, the double tetrahedron has 6 indirect symmetries and hence it has 12 symmetries altogether.



To find these symmetries we could first find all the direct symmetries, and then compose them all in turn with the indirect symmetry mentioned above. However, there is a slightly simpler way to proceed for this particular solid. We can observe that each symmetry of the equilateral triangle with vertices labelled 1, 2 and 3 in the middle of the solid gives a symmetry of the whole solid, and that each of these symmetries, when composed with the reflection in the plane in which this triangle lies, gives another symmetry of the whole solid.

The symmetries of the first type are represented by the permutations in the first column below. To obtain the permutations that represent the symmetries of the second type, we compose each of the symmetries in the first column with the transposition $(4\ 5)$, which represents the reflection in the horizontal plane containing the triangle. This gives the symmetries in the second column below. Since we have found 12 different symmetries, these are all the symmetries of the double tetrahedron.

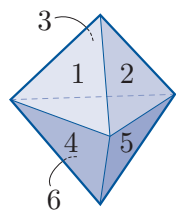
The symmetries of the double tetrahedron are represented by the following permutations in S_5 .

e	$(4\ 5)$
$(1\ 2)$	$(1\ 2)(4\ 5)$
$(1\ 3)$	$(1\ 3)(4\ 5)$
$(2\ 3)$	$(2\ 3)(4\ 5)$
$(1\ 2\ 3)$	$(1\ 2\ 3)(4\ 5)$
$(1\ 3\ 2)$	$(1\ 3\ 2)(4\ 5)$

In the next exercise you are asked to find the symmetries of the double tetrahedron when its face locations are labelled.

Exercise B104

Write down the permutations in S_6 that represent the symmetries of the double tetrahedron when its face locations are labelled as shown below.



Hint: You can proceed as in Worked Exercise B39, though finding the composites involves a little more work.

In Worked Exercise B39 we represented the symmetry group of the double tetrahedron as a subgroup of S_5 , by labelling the vertex locations, and then in Exercise B104 we represented the same symmetry group as a subgroup of S_6 , by labelling the face locations. We could also represent the same symmetry group as a subgroup of S_9 by labelling the edge locations, as shown in Figure 10.

This illustrates that different permutation groups representing the same symmetry group may involve different numbers of symbols being permuted. The orders of these different permutation groups (that is, the number of elements that they contain) must be the same, of course.

The material in the blue box below is rather more complicated than in most of them, but you may find it interesting. Remember that the material in all the blue boxes is optional.

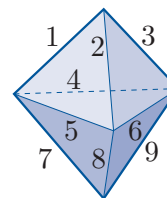


Figure 10 The double tetrahedron with its edges labelled

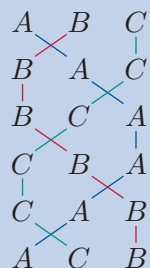
Permutations and bell ringing

The bells of a church ring with different pitches. Each bell is rung by pulling a rope to swing it, but there is a minimum time interval between successive strokes of the same bell, so bell ringers cannot play tunes. Instead, they often aim to ring a sequence in which each bell rings exactly once, then another such sequence with the bells in a different order, then another, and so on, until they have rung a number of such sequences, all different, in some sort of pattern. Ideally the pattern should be one that is not too hard for the bell ringers to remember. The order of the sequences in the pattern must be such that each bell changes by at most one place from each sequence to the next, to avoid the interval between successive rings of the same bell being less than the minimum possible.

For example, suppose there are three bells, A , B and C . Then there are six possible sequences of bells (since $3! = 6$), as follows:

ABC , ACB , BAC , BCA , CAB , CBA .

Here is a suitable order for ringing the three bells, which includes all six possible sequences; such an order is known as an *extent*. The coloured lines trace the changes in place of each bell. You can see that each bell changes by at most one place from each sequence to the next.









Church bells



Bell ringers

For larger numbers of bells it becomes harder to find an extent, but we can use group theory to help us do it.

Here is how we can think of the extent for three bells above in terms of group theory. To get from the first sequence to the second, we swap the bells in places 1 and 2; that is, we apply the transposition of places (1 2). In fact, the only permutations of places allowed from one sequence to the next in the extent are the transpositions (1 2) and (2 3), since anything else involves a bell changing by more than one place. In the extent these two transpositions are applied alternately, as shown below.

Sequence of bells	Transposition applied
	
	(1 2)
	(2 3)
	(1 2)
	(2 3)
	(1 2)

The second sequence of the extent is obtained from the first sequence by applying the transposition (1 2), but we can also determine how each of the other sequences is obtained *from the first sequence*, as follows.


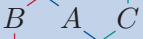


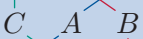

The third sequence is obtained by applying the transposition (1 2) followed by the transposition (2 3); that is, by applying the permutation

$$(2\ 3) \circ (1\ 2) = (1\ 3\ 2).$$






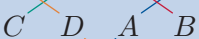


Similarly, the fourth sequence is obtained by applying (1 2) followed by (2 3) followed by (1 2); that is, by applying

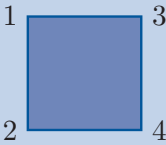
$$(1\ 2) \circ (2\ 3) \circ (1\ 2) = (1\ 3).$$

The table below shows the permutation of places obtained in this way corresponding to each sequence in the extent. The six permutations of places are all different, corresponding to the fact that the sequences they give are all different. Thus the six permutations of places are the six elements of the symmetric group S_3 .

Sequence of bells	Transposition applied	Permutation from start
		e
	$(1\ 2)$	$(1\ 2)$
	$(2\ 3)$	$(1\ 3\ 2)$
	$(1\ 2)$	$(1\ 3)$
	$(2\ 3)$	$(1\ 2\ 3)$
	$(1\ 2)$	$(2\ 3)$

For four bells, the only permutations of places allowed from one sequence to the next are $(1\ 2)$, $(2\ 3)$, $(3\ 4)$ and $(1\ 2)(3\ 4)$. The table below shows a partial extent for four bells, in which the permutations $(2\ 3)$ and $(1\ 2)(3\ 4)$ are applied alternately. Its pattern is similar to that of the extent for three bells above, as you can see from the coloured lines. However, it includes only eight of the $4! = 24$ possible sequences of four bells. (Applying $(2\ 3)$ to the final sequence gives the first sequence again.) The corresponding eight permutations of places are in fact the elements of the group $S(\square)$, when the square is labelled as shown on the right below.

Sequence of bells	Permutation applied	Permutation from start
		e
	$(1\ 2)(3\ 4)$	$(1\ 2)(3\ 4)$
	$(2\ 3)$	$(1\ 3\ 4\ 2)$
	$(1\ 2)(3\ 4)$	$(1\ 4)$
	$(2\ 3)$	$(1\ 4)(2\ 3)$
	$(1\ 2)(3\ 4)$	$(1\ 3)(2\ 4)$
	$(2\ 3)$	$(1\ 2\ 4\ 3)$
	$(1\ 2)(3\ 4)$	$(2\ 3)$



In Book E you can see how the idea of *cosets* can be used to extend the partial extent above to give a full extent for four bells, that is, one that includes all 24 sequences.

For larger numbers of bells – churches commonly have six bells or eight bells – it would take a long time to ring a full extent: about 25 minutes for six bells, and about 24 hours for eight bells! So bell ringers usually ring partial extents. However, a full extent on eight bells was rung by a single team at Loughborough Bell Foundry in 1963, taking about 18 hours.

(Note that usually numbers are used to represent bells and letters to represent places, but in the discussion above these notations have been swapped to fit more naturally with the theory in this unit.)

3 Even and odd permutations

In this section you will see that, for any integer $n \geq 2$, the set S_n of all permutations of the set $\{1, 2, 3, \dots, n\}$ splits naturally into two classes of permutations, known as *even* permutations and *odd* permutations. Before you can see why, you need to learn how to express every permutation in a particular way – namely as a composite of transpositions.

3.1 Expressing a permutation as a composite of transpositions

As you saw in the previous section, a **transposition** is a 2-cycle, that is, a permutation that interchanges two symbols and leaves all the others fixed. For example, in the symmetric group S_4 , which consists of all permutations of the set $\{1, 2, 3, 4\}$, the transposition $(2\ 4)$ interchanges the symbols 2 and 4 and leaves the symbols 1 and 3 fixed.

In the next exercise you are asked to find some composites of transpositions. You saw how to compose permutations in Subsection 1.2. Remember that when you compose permutations (and transpositions in particular), the order of composition is important. For example,

$$(1\ 3) \circ (1\ 2) = (1\ 2\ 3),$$

whereas

$$(1\ 2) \circ (1\ 3) = (1\ 3\ 2).$$

(In contrast, the order of the cycles in the cycle form of a permutation does not matter, but this is because those cycles are *disjoint*.) Remember, too, that we compose permutations starting with the right-most permutation. For example, the composite permutation

$$(1\ 4) \circ (1\ 3) \circ (1\ 2)$$

means

$$(1\ 2) \text{ followed by } (1\ 3) \text{ followed by } (1\ 4).$$

Exercise B105

- (a) Determine the following composites of transpositions in S_4 .
 (i) $(1\ 4) \circ (1\ 2)$ (ii) $(1\ 3) \circ (1\ 2) \circ (1\ 4)$ (iii) $(3\ 1) \circ (3\ 4) \circ (3\ 2)$
- (b) Can you see a pattern in the solution to part (a)? If so, express each of the cycles $(1\ 4\ 3)$ and $(1\ 4\ 3\ 2)$ as a composite of transpositions.

The pattern discovered in the solution to Exercise B105 is generalised in the following strategy. A justification of why the strategy works is given at the end of this subsection.

Strategy B10

To express a cycle $(a_1\ a_2\ a_3\ \dots\ a_r)$ as a composite of transpositions, do the following.

Write the transpositions

$$(a_1\ a_2), (a_1\ a_3), (a_1\ a_4), \dots, (a_1\ a_r)$$

in reverse order and form their composite. That is,

$$(a_1\ a_2\ a_3\ \dots\ a_r) = (a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \dots \circ (a_1\ a_3) \circ (a_1\ a_2).$$

Worked Exercise B40

Express the following cycles in S_5 as composites of transpositions.

- (a) $(2\ 4\ 3\ 5)$ (b) $(1\ 3\ 2\ 5\ 4)$

Solution

 Use Strategy B10. 

$$(a) \quad (2\ 4\ 3\ 5) = (2\ 5) \circ (2\ 3) \circ (2\ 4)$$

$$(b) \quad (1\ 3\ 2\ 5\ 4) = (1\ 4) \circ (1\ 5) \circ (1\ 2) \circ (1\ 3)$$

Exercise B106

Use Strategy B10 to express the following cycles in S_7 as composites of transpositions.

- (a) $(1\ 5\ 2\ 7\ 3)$ (b) $(2\ 3\ 7\ 5\ 4\ 6)$ (c) $(1\ 2\ 3\ 4\ 5\ 6\ 7)$

Notice that Strategy B10 does not produce a *unique* expression for a cycle as a composite of transpositions. For instance, $(2\ 4\ 3\ 5)$ and $(4\ 3\ 5\ 2)$ are the same 4-cycle, but with a different symbol in the first position. The strategy gives the following alternative expressions as composites of transpositions:

$$\begin{aligned}(2\ 4\ 3\ 5) &= (2\ 5) \circ (2\ 3) \circ (2\ 4) \\ &= (4\ 3\ 5\ 2) = (4\ 2) \circ (4\ 5) \circ (4\ 3).\end{aligned}$$

However, for any particular cycle, the strategy always produces an expression with the same *number* of transpositions, as illustrated in the next exercise.

Exercise B107

How many transpositions do you obtain if you use Strategy B10 to express each of the following as a composite of transpositions?

- (a) A 4-cycle. (b) A 5-cycle. (c) An r -cycle (for $r \geq 2$).

Although Strategy B10 is a method for expressing any *cycle* as a composite of transpositions, we can use it to express any *permutation* as a composite of transpositions, as demonstrated next.

Worked Exercise B41

Express the permutation $(1\ 9)(2\ 3\ 6\ 7)(4\ 8\ 5)$ as a composite of transpositions.

Solution

 Use the fact that the permutation is equal to the composite of its disjoint cycles, and apply Strategy B10 to each of the cycles. 

$$\begin{aligned}(1\ 9)(2\ 3\ 6\ 7)(4\ 8\ 5) &= (1\ 9) \circ (2\ 3\ 6\ 7) \circ (4\ 8\ 5) \\ &= (1\ 9) \circ (2\ 7) \circ (2\ 6) \circ (2\ 3) \circ (4\ 5) \circ (4\ 8).\end{aligned}$$

Thus we have the following theorem.

Theorem B56

Every permutation can be expressed as a composite of transpositions.

Proof A permutation in cycle form can be expressed as a composite of transpositions by applying Strategy B10 to each of its cycles. ■

Exercise B108

Express each of the following permutations in S_8 as a composite of transpositions.

(a) $(1\ 8\ 3)(2\ 6\ 5\ 7)$ (b) $(1\ 7)(2\ 6\ 8)(3\ 4\ 5)$

To end this subsection, here is a proof that Strategy B10 works.

Theorem B57

If a_1, a_2, \dots, a_r are symbols (where $r \geq 2$), then the composite of transpositions

$$(a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \cdots \circ (a_1\ a_3) \circ (a_1\ a_2)$$

is equal to the cycle

$$(a_1\ a_2\ a_3 \dots a_r).$$

Proof We can check this by finding the cycle form of the composite of transpositions in the usual way.

First we consider the symbol a_1 . The first transposition $(a_1\ a_2)$ maps a_1 to a_2 and the remaining transpositions map a_2 to itself, so the composite maps a_1 to a_2 .

Now we consider any symbol a_s where $2 \leq s \leq r-1$ (we consider a_r later). We see that

- each of the transpositions

$$(a_1\ a_2), (a_1\ a_3), \dots, (a_1\ a_{s-1})$$

maps a_s to itself

- the next transposition $(a_1\ a_s)$ maps a_s to a_1
- then the next transposition $(a_1\ a_{s+1})$ maps a_1 to a_{s+1}
- and each of the remaining transpositions

$$(a_1\ a_{s+2}), \dots, (a_1\ a_r)$$

maps a_{s+1} to itself.

Hence the composite maps a_s to a_{s+1} .

It remains to find the image of a_r . The symbol a_r is mapped to itself by all the transpositions except the final one $(a_1\ a_r)$, which maps a_r to a_1 . Hence the composite maps a_r to a_1 .

Thus the cycle form of the composite of transpositions is the cycle $(a_1\ a_2\ a_3 \dots a_r)$, as required. ■

3.2 Parity of a permutation

A permutation can be expressed as a composite of transpositions in many different ways, not all of which arise from the method that you saw in the previous subsection. The different ways do not all contain the same number of transpositions. For example, here are a few ways of expressing the 3-cycle $(1\ 2\ 3)$ in S_3 as a composite of transpositions:

$$\begin{aligned}(1\ 2\ 3) &= (1\ 3) \circ (1\ 2) \\ &= (1\ 2) \circ (2\ 3) \\ &= (2\ 3) \circ (1\ 3) \\ &= (2\ 3) \circ (1\ 2) \circ (2\ 3) \circ (1\ 2) \\ &= (1\ 2) \circ (2\ 3) \circ (3\ 1) \circ (3\ 2) \circ (2\ 1) \circ (2\ 3).\end{aligned}$$

You can check that each of these expressions is equal to $(1\ 2\ 3)$ by composing the transpositions. Notice that each of the expressions involves an *even* number of transpositions.

It turns out that if a permutation can be expressed in *one* way as a composite of an even number of transpositions, then *every* way of expressing it as a composite of transpositions involves an even number of transpositions. Similarly, if a permutation can be expressed in *one* way as a composite of an odd number of transpositions, then *every* way of expressing it as a composite of transpositions involves an odd number of transpositions. In other words, we have the following result.

Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

A proof of this theorem is given at the end of this section, in Subsection 3.4.

The theorem tells us that permutations can be classified into two kinds, which we call *odd* permutations and *even* permutations, as defined below.

Definitions

A permutation is **even** if it can be expressed as a composite of an even number of transpositions.

A permutation is **odd** if it can be expressed as a composite of an odd number of transpositions.

The evenness/oddness of a permutation is called its **parity**.

For example, the permutation $(1\ 2\ 3\ 4)$ in the group S_4 is odd, since

$$(1\ 2\ 3\ 4) = (1\ 4) \circ (1\ 3) \circ (1\ 2).$$

This equation shows that $(1\ 2\ 3\ 4)$ can be expressed in one way (and therefore in every way) as a composite of an odd number of transpositions.

On the other hand, the permutation $(1\ 3\ 5\ 4\ 2)$ in S_5 is even, since

$$(1\ 3\ 5\ 4\ 2) = (1\ 2) \circ (1\ 4) \circ (1\ 5) \circ (1\ 3).$$

This equation shows that $(1\ 3\ 5\ 4\ 2)$ can be expressed in one way (and therefore in every way) as a composite of an even number of transpositions.

Note that a transposition is an odd permutation, since it is a composite of one transposition, namely itself.

The identity permutation e is an even permutation, because it can be expressed as a composite of two transpositions, such as

$$e = (1\ 2) \circ (1\ 2).$$

(Alternatively, you may regard e as a composite of no transpositions; and 0 is even.)

Also, an r -cycle is a composite of $r - 1$ transpositions, as found in the solution to Exercise B107(c), so an r -cycle is an even permutation when r is odd and an odd permutation when r is even.

These facts are collected together in the following theorem.

Theorem B59

In the group S_n ,

$$\text{an } r\text{-cycle is } \begin{cases} \text{an even permutation,} & \text{if } r \text{ is odd,} \\ \text{an odd permutation,} & \text{if } r \text{ is even.} \end{cases}$$

In particular, a transposition is an odd permutation and the identity permutation is an even permutation.

Exercise B109

- (a) Determine whether each of the following permutations in S_6 is even or odd:

$$(1\ 2\ 5\ 3), \quad (1\ 6\ 2\ 5\ 4).$$

- (b) Use the solution to Exercise B108 to classify each of the following permutations in S_8 as even or odd:

$$(1\ 8\ 3)(2\ 6\ 5\ 7), \quad (1\ 7)(2\ 6\ 8)(3\ 4\ 5).$$

- (c) Determine the parity of the permutation $(1\ 8\ 2\ 7\ 6)(3\ 5\ 9\ 4)$.

Notice that if f and g are permutations in S_n , then the parity of $g \circ f$ can be deduced directly from the parities of f and g . For example, if f and g are both even, then we can replace each of the permutations f and g in $g \circ f$ by a composite of an even number of transpositions: this gives an expression for $g \circ f$ as an even number of transpositions, so $g \circ f$ is even.

In general, for any permutations f and g in S_n , we can deduce the parity of $g \circ f$ from the parities of f and g by using the fact that the addition of even and odd integers has the pattern in the table below.

+	even	odd
even	even	odd
odd	odd	even

Thus if f and g are both even or both odd, then $g \circ f$ is even, whereas if f and g have different parities, then $g \circ f$ is odd.


These observations enable us to find the parity of a permutation without having to write out any transpositions.

Worked Exercise B42

Determine the parity of the following permutation in S_9 :

$$(1\ 2\ 3\ 4)(5\ 6)(7\ 8\ 9).$$

Solution

 Use the fact that the permutation is equal to the composite of its disjoint cycles:

$$(1\ 2\ 3\ 4)(5\ 6)(7\ 8\ 9) = (1\ 2\ 3\ 4) \circ (5\ 6) \circ (7\ 8\ 9).$$

Find the parity of each cycle, using the fact that a cycle of even length is odd and a cycle of odd length is even.

$$\underbrace{(1\ 2\ 3\ 4)}_{\text{odd}} \circ \underbrace{(5\ 6)}_{\text{odd}} \circ \underbrace{(7\ 8\ 9)}_{\text{even}}$$

Deduce the parity of the composite permutation. 

The parity of the permutation is

$$\text{odd} + \text{odd} + \text{even} = \text{even}.$$

In Worked Exercise B42 we worked out the parity of a composite of disjoint cycles by finding the parity of each cycle and deducing the overall parity. We can use the same method to work out the parity of any composite of permutations – it does not matter whether the cycles that form the composite are disjoint or not.

Worked Exercise B43

Determine the parity of the following composite in S_6 :

$$(1\ 2\ 4)(3\ 5) \circ (1\ 3)(2\ 4\ 6\ 5) \circ (1\ 5\ 2\ 6\ 3\ 4).$$

Solution

 We have

$$\begin{aligned} & (1\ 2\ 4)(3\ 5) \circ (1\ 3)(2\ 4\ 6\ 5) \circ (1\ 5\ 2\ 6\ 3\ 4) \\ &= (1\ 2\ 4) \circ (3\ 5) \circ (1\ 3) \circ (2\ 4\ 6\ 5) \circ (1\ 5\ 2\ 6\ 3\ 4). \end{aligned}$$

The given composite is

$$\text{even} + \text{odd} + \text{odd} + \text{odd} + \text{odd} = \text{even}.$$

The ideas illustrated in Worked Exercises B42 and B43 are collected in the following general strategy.

Strategy B11

To determine the parity of a permutation, do the following.

1. Express the permutation as a composite of cycles (either disjoint or not).
2. Find the parity of each cycle, using the rule:

$$\text{an } r\text{-cycle is } \begin{cases} \text{even,} & \text{if } r \text{ is odd,} \\ \text{odd,} & \text{if } r \text{ is even.} \end{cases}$$

3. Combine the even and odd parities using the following table.

+	even	odd
even	even	odd
odd	odd	even

Exercise B110

Use Strategy B11 to determine the parity of each of the following composite permutations in S_5 .

(a) $(1\ 2\ 4)(3\ 5) \circ (1\ 5\ 2)$ (b) $(1\ 2\ 4) \circ (1\ 3)(2\ 5\ 4) \circ (1\ 2\ 3\ 4)$

You may have noticed from Worked Exercise B43 and Exercise B110 that steps 2 and 3 of Strategy B11 together amount to the following rule: if the number of cycles of *even* length (that is, the number of cycles that are *odd* permutations) is

even, then the permutation is even,
odd, then the permutation is odd.

However, it is probably more helpful to remember the steps of Strategy B11 rather than this rule.

In the discussion above you saw how to deduce the parity of a composite permutation $g \circ f$ from the parity of the individual permutations f and g . We can also deduce the parity of an inverse permutation f^{-1} from the parity of the original permutation f , using the following simple result.

Theorem B60

A permutation and its inverse have the same parity.

Proof A permutation and its inverse have the same cycle structure, because we obtain the inverse by writing each cycle of the permutation in reverse order. Since it is the cycle structure alone that determines the parity of a permutation, it follows that a permutation and its inverse have the same parity. ■

An alternative way to prove Theorem B60 is to consider the parities of the permutations in the equation $f \circ f^{-1} = e$. We know that e is even, so f and f^{-1} must have the same parity, because otherwise $f \circ f^{-1}$ would be the composite of an even permutation and an odd permutation and hence would be odd.

3.3 The alternating group A_n

We denote the set of all *even* permutations of the set of symbols $\{1, 2, 3, \dots, n\}$ by A_n . Thus A_n is a subset of S_n .

In fact, A_n is a *subgroup* of S_n , as shown below.

Theorem B61

The set A_n of all even permutations of the set $\{1, 2, 3, \dots, n\}$ is a subgroup of the symmetric group S_n .

Proof We check that the three subgroup properties SG1, SG2 and SG3 hold. (These are given in Theorem B24 of Unit B2.)

SG1 Closure We have seen that the composite of two even permutations is an even permutation. That is, for all $f, g \in A_n$, the composite $g \circ f$ is in A_n .

SG2 Identity The identity permutation e is even, so e is in A_n .

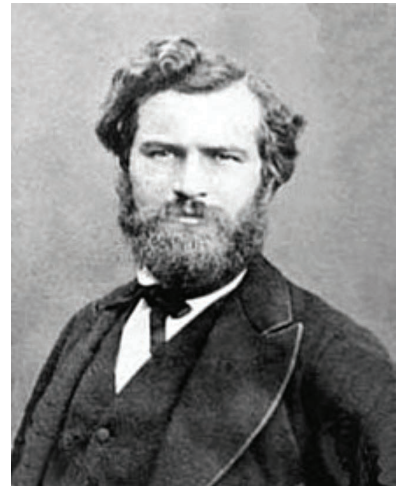
SG3 Inverses We have seen that a permutation and its inverse have the same parity. In particular, the inverse of an even permutation is itself an even permutation. That is, for each $f \in A_n$, its inverse f^{-1} is in A_n .

Thus A_n satisfies the three subgroup properties, and so is a subgroup of S_n . ■

Definition

The group A_n of all even permutations of $\{1, 2, \dots, n\}$ is called the **alternating group of degree n** .

The term *alternating group* was introduced in 1873 by Camille Jordan (1838–1922), whose contribution to group theory has already been mentioned in Unit B2. Jordan, who studied mathematics at the École Polytechnique in Paris, trained as an engineer and continued in that profession, at least by name, until 1885. It was while working as an engineer that he did most of his mathematical research, publishing papers on a wide variety of topics ranging from topology to mechanics, as well as in group theory, the subject in which he was seen as the undisputed master for forty years.



Camille Jordan

Exercise B111

List the elements of the alternating group A_3 , and hence state the order of this group. (The elements of the symmetric group S_3 were found in Worked Exercise B36.)

Now let us find the elements of the alternating group A_4 . The cycle structures in the symmetric group S_4 (found in the solution to Exercise B92) are

$$e, \quad (- -), \quad (- - -), \quad (- - - -), \quad (- -)(- -).$$

Their corresponding parities are, respectively,

$$\text{even}, \quad \text{odd}, \quad \text{even}, \quad \text{odd}, \quad \text{odd} + \text{odd} = \text{even}.$$

So the possible cycle structures in A_4 are

$$e, \quad (- - -), \quad (- -)(- -).$$

The symbols in the cycles are from the set $\{1, 2, 3, 4\}$.

For the cycle structure $(- - -)$, there are four choices for the three symbols that appear in the 3-cycle, namely $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$ and $\{2, 3, 4\}$. For each of these four choices of symbols, there are two 3-cycles containing the three symbols. For example, the two 3-cycles containing the symbols 1, 2 and 3 are $(1\ 2\ 3)$ and $(1\ 3\ 2)$, because we can assume that the smallest symbol, 1, is placed first in each cycle, and there are then two different ways to place the other two symbols in the other two places.

There are three elements of A_4 with the cycle structure $(- -)(- -)$, namely $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$, because there are three choices for the symbol that is in the same transposition as the symbol 1, and the other two symbols must then be in the other transposition.

Thus the elements of A_4 are as listed in Table 2.

Table 2 The elements of the alternating group A_4

Cycle structure	Number of permutations	Elements of A_4
e	1	e
$(- - -)$	8	$(1\ 2\ 3), (1\ 3\ 2),$ $(1\ 2\ 4), (1\ 4\ 2),$ $(1\ 3\ 4), (1\ 4\ 3),$ $(2\ 3\ 4), (2\ 4\ 3)$
$(- -)(- -)$	3	$(1\ 2)(3\ 4),$ $(1\ 3)(2\ 4),$ $(1\ 4)(2\ 3)$

Table 2 shows that the order of the alternating group A_4 is $1 + 8 + 3 = 12$. This is exactly half of the order of the symmetric group S_4 , which is $4! = 24$. Similarly, as you saw in Exercise B111, the order of the alternating group A_3 is 3, and this is exactly half of the order of the symmetric group S_3 , which is $3! = 6$. In fact, for every integer $n \geq 2$ the order of the alternating group A_n is half of the order of the symmetric group S_n . In other words, since the symmetric group S_n has order $n!$ (by Theorem B53), the alternating group A_n has order $\frac{1}{2}(n!)$. This is stated and proved below.

Theorem B62

For each integer $n \geq 2$, the alternating group A_n has order $\frac{1}{2}(n!)$.

Proof Suppose that S_n has r even permutations and s odd permutations. We will establish that $r = s$ by showing that both $r \leq s$ and $r \geq s$.

To prove that $r \leq s$, suppose that the r even permutations in S_n are $f_1, f_2, f_3, \dots, f_r$, and consider the r permutations

$$(1\ 2) \circ f_1, \quad (1\ 2) \circ f_2, \quad (1\ 2) \circ f_3, \quad \dots, \quad (1\ 2) \circ f_r.$$

These permutations are all odd, since each is the composite of a transposition with an even permutation.

Moreover, these r permutations are distinct, because if

$$(1\ 2) \circ f_i = (1\ 2) \circ f_j,$$

then, by the Left Cancellation Law in the group S_n ,

$$f_i = f_j.$$

So we have found r odd permutations in S_n . It follows that s , the total number of odd permutations, is greater than or equal to r ; that is, $r \leq s$.

A similar argument shows that if the s odd permutations in S_n are $g_1, g_2, g_3, \dots, g_s$, then the s permutations

$$(1\ 2) \circ g_1, \quad (1\ 2) \circ g_2, \quad (1\ 2) \circ g_3, \quad \dots, \quad (1\ 2) \circ g_s$$

are distinct even permutations in S_n , so $r \geq s$.

It follows that $r = s$, so exactly half the permutations in S_n are even.

Since S_n has order $n!$, it follows that A_n has order $\frac{1}{2}(n!)$. ■

3.4 Proof of the Parity Theorem (optional)

This subsection provides a proof of the Parity Theorem. The material in this subsection will not be assessed.

Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

The proof of the Parity Theorem depends on considering the number of cycles in the cycle form of a permutation, including any 1-cycles, which are usually omitted from the cycle form. We will refer to this number as the *cycle number* of the permutation. For example, the permutation

$$(1\ 4\ 3)(2\ 5)(6\ 7\ 8\ 9)$$

in S_9 has cycle number 3, and the permutation

$$(1\ 4\ 3)(2\ 5)(6\ 7)$$

in S_9 has cycle number 5, since

$$(1\ 4\ 3)(2\ 5)(6\ 7) = (1\ 4\ 3)(2\ 5)(6\ 7)(8)(9).$$

The main fact needed for the proof is as follows. Suppose that f is a permutation in S_n and $t = (a\ b)$ is a transposition in S_n . Then the cycle numbers of f and $t \circ f$ always differ by 1. If the symbols a and b lie in the same cycle in the cycle form of f , then composing with $t = (a\ b)$ cuts this cycle into two cycles; whereas if they lie in different cycles (possibly 1-cycles), then composing with $t = (a\ b)$ joins these two cycles into one cycle. This is illustrated in the following exercise.

Exercise B112

For each of the following permutations f in S_7 , write down the cycle number of f . Then find $t \circ f$ in cycle form, where t is the transposition $(1\ 2)$, and write down the cycle number of $t \circ f$.

- (a) $(1\ 4\ 5\ 2\ 3\ 6\ 7)$ (b) $(1\ 4\ 3)(2\ 6\ 5\ 7)$ (c) $(1\ 2\ 7\ 3)(4\ 6)$
 (d) $(1\ 5\ 3)(2\ 4)(6\ 7)$

Here is a proof that the fact illustrated by Exercise B112 is true in general. (We refer to the result below as a *lemma* because it is an intermediate step in the proof of our main result, the Parity Theorem.)

Lemma B63

If f is a permutation in S_n and t is a transposition in S_n , then the cycle numbers of f and $t \circ f$ differ by 1.

Proof Let f be a permutation in S_n and let $t = (a\ b)$ be a transposition in S_n .

First suppose that the symbols a and b lie in the same cycle in the cycle form of f . Then we may write

$$f = (a\ x_1\ x_2\ \dots\ x_r\ b\ y_1\ y_2\ \dots\ y_s)f_1f_2 \cdots f_m,$$

where x_1, x_2, \dots, x_r and y_1, y_2, \dots, y_s are symbols from $\{1, 2, \dots, n\}$, and f_1, f_2, \dots, f_m are cycles in S_n that are disjoint from the cycle containing

a and b . If we use the usual method for composing permutations (starting with the symbol a), we obtain

$$\begin{aligned} t \circ f &= (a \ b) \circ (a \ x_1 \ x_2 \ \dots \ x_r \ b \ y_1 \ y_2 \ \dots \ y_s) f_1 f_2 \cdots f_m \\ &= (a \ x_1 \ x_2 \ \dots \ x_r) (b \ y_1 \ y_2 \ \dots \ y_s) f_1 f_2 \cdots f_m. \end{aligned}$$

So the cycle number of $t \circ f$ is 1 greater than that of f . This happens even if the cycle containing a and b is of the form $(a \ b \ y_1 \ y_2 \ \dots \ y_s)$ or $(a \ x_1 \ x_2 \ \dots \ x_r \ b)$ or simply $(a \ b)$. (Also, there may be no cycles f_1, f_2, \dots, f_m other than the cycle containing a and b in the cycle form of f , but this is of no consequence in the argument.)

Next suppose that a and b lie in different cycles of f . Then we may write

$$f = (a \ x_1 \ x_2 \ \dots \ x_r) (b \ y_1 \ y_2 \ \dots \ y_s) f_1 f_2 \cdots f_m,$$

where x_1, x_2, \dots, x_r and y_1, y_2, \dots, y_s are symbols from $\{1, 2, \dots, n\}$ and f_1, f_2, \dots, f_m are cycles in S_n that are disjoint from the cycles containing a and b . We now use the usual method for composing permutations (starting with the symbol a) to obtain

$$\begin{aligned} t \circ f &= (a \ b) \circ (a \ x_1 \ x_2 \ \dots \ x_r) (b \ y_1 \ y_2 \ \dots \ y_s) f_1 f_2 \cdots f_m \\ &= (a \ x_1 \ x_2 \ \dots \ x_r \ b \ y_1 \ y_2 \ \dots \ y_s) f_1 f_2 \cdots f_m. \end{aligned}$$

So the cycle number of $t \circ f$ is 1 less than that of f . This happens even if the cycles containing a and b are of the forms $(a)(b \ y_1 \ y_2 \ \dots \ y_s)$ or $(a \ x_1 \ x_2 \ \dots \ x_r)(b)$ or simply $(a)(b)$. (Again, there may be no cycles f_1, f_2, \dots, f_m other than the cycles containing a and b in the cycle form of f ; and again this is of no consequence in the argument.)

Thus in both cases the cycle numbers of f and $t \circ f$ differ by 1, as claimed. ■

We can now prove the Parity Theorem.

Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

Proof Let f be a permutation in S_n . Suppose that f can be expressed as a composite of r transpositions as follows:

$$f = t_r \circ t_{r-1} \circ \cdots \circ t_2 \circ t_1.$$

The cycle form of f can be found by first composing t_2 with t_1 , then t_3 with the resulting permutation, and so on. There are $r - 1$ such compositions to be performed and, at each of these, the cycle number either increases by 1 or decreases by 1, by Lemma B63. Suppose that it increases i times and therefore decreases $r - 1 - i$ times. The cycle number of t_1 is $n - 1$ (since t_1 has $n - 1$ cycles: it has one 2-cycle and all its other cycles are 1-cycles), so it follows that the cycle number c of f is given by

$$c = (n - 1) + i - (r - 1 - i),$$

that is,

$$c = n + 2i - r.$$

Rearranging this equation, we obtain

$$r = n - c + 2i.$$

It follows that if $n - c$ is odd, then the number r of transpositions is odd; whereas if $n - c$ is even, then r is even. Since the numbers n and c are fixed for the permutation f (they are the number of symbols being permuted, and the cycle number of f , respectively), this proves the result. ■

Notice that the proof above gives us an alternative way of determining the parity of a permutation in cycle form: the parity is even if $n - c$ is even, and odd if $n - c$ is odd, where n is the number of symbols being permuted, and c is the cycle number of the permutation.

4 Conjugacy in S_n

In this section you will learn about the important idea of *conjugacy* in symmetric groups. In Book E *Group theory 2* you will see that this idea can be extended to all groups.

4.1 Conjugate permutations in S_n

To illustrate the idea of conjugacy we will start by considering permutations that represent the symmetries of the square. You saw in Subsection 2.4 that when the vertex locations of the square are labelled in the usual way, as shown in Figure 11, we can represent the eight symmetries of the square by the following eight permutations in cycle form.

Rotations	Reflections
e	$(1\ 4)(2\ 3)$
$(1\ 2\ 3\ 4)$	$(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$
$(1\ 4\ 3\ 2)$	$(1\ 3)$

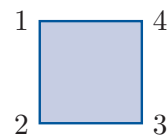


Figure 11 The square with its usual vertex labelling

Of course, the permutations that represent the symmetries of the square depend on the way that we label the vertex locations. If we relabel the vertex locations, then we obtain different permutations representing the symmetries.

For example, suppose that we use the same four labels 1, 2, 3 and 4, but relabel the vertex locations by interchanging the symbols 2 and 3, as shown in Figure 12. That is, we rearrange the labels using the transposition $(2\ 3)$.

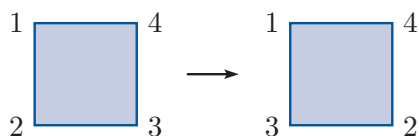


Figure 12 Relabelling the square by interchanging the labels 2 and 3

A quick way to obtain the permutations that represent the symmetries of the square with this new labelling is to take the list of permutations above and replace every occurrence of the symbol 2 with the symbol 3 and vice versa; that is, we ‘rename’ the symbols using the transposition $(2\ 3)$. So, for example, the rotation $(1\ 2\ 3\ 4)$ becomes the rotation $(1\ 3\ 2\ 4)$, and the reflection $(1\ 4)(2\ 3)$ becomes the reflection $(1\ 4)(3\ 2)$, and so on. With the new labelling, the full list of permutations that represent the eight symmetries of the square is as follows.

Rotations	Reflections
e	$(1\ 4)(3\ 2)$
$(1\ 3\ 2\ 4)$	$(3\ 4)$
$(1\ 2)(3\ 4)$	$(1\ 3)(2\ 4)$
$(1\ 4\ 2\ 3)$	$(1\ 2)$

The first reflection in the list above, $(1\ 4)(3\ 2)$, is not written in the usual way (that is, with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order). If we wish to write it in the usual way, then we obtain the following list of permutations representing the symmetries of the square.

Rotations	Reflections
e	$(1\ 4)(2\ 3)$
$(1\ 3\ 2\ 4)$	$(3\ 4)$
$(1\ 2)(3\ 4)$	$(1\ 3)(2\ 4)$
$(1\ 4\ 2\ 3)$	$(1\ 2)$

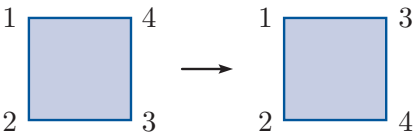
In the next exercise you are asked to write down the permutations that represent the symmetries of the square when the vertices are relabelled with the symbols 1, 2, 3 and 4 in two other ways.

Exercise B113

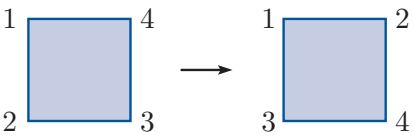
The permutations that represent the symmetries of the square when it is labelled in the usual way, as shown in Figure 11, are repeated below.

Rotations	Reflections
e	$(1\ 4)(2\ 3)$
$(1\ 2\ 3\ 4)$	$(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$
$(1\ 4\ 3\ 2)$	$(1\ 3)$

- (a) By starting with the list of permutations above and replacing symbols as required, find the permutations that represent the symmetries of the square when it is relabelled by interchanging the labels 3 and 4, that is, by using the transposition $(3\ 4)$, as shown below.



- (b) Repeat part (a) for when the vertex locations of the square are relabelled using the permutation $(2\ 3\ 4)$, as shown below.



We have now found various different ways to represent $S(\square)$ as a subgroup of the symmetric group S_4 , by relabelling the vertices of the square with the symbols 1, 2, 3 and 4 in different ways. In doing so, we have found three different, but related, subgroups of S_4 (the two subgroups found in Exercise B113 are actually the same subgroup). We will return to these ideas of related subgroups in the next subsection, but first we need to look more closely at the ‘symbol renaming’ process that we used to obtain new representations of $S(\square)$ from the original representation. We will consider the effect of this process on a single permutation.

The process, which you carried out several times in Exercise B113, can be described as follows. We take a permutation, say x , and we rename its symbols using another permutation, say g , to obtain a third permutation, say y . We carried out this process with permutations of the set $\{1, 2, 3, 4\}$, but we can carry it out in the same way with permutations of any set of symbols.

You might expect that when this process is carried out there will be some sort of algebraic relationship between the permutations x , g and y , and indeed there is. We will now work out what it is.

Let us look at an example of the process being carried out with permutations of the set of symbols $\{1, 2, 3, 4, 5\}$; that is, permutations in S_5 . Suppose that we start with the permutation $x = (1\ 2\ 5)(3\ 4)$ and rename its symbols using the permutation $g = (1\ 3\ 5\ 4)$, as illustrated below:

$$\begin{array}{ccccccc} x & = & (1\ 2\ 5)(3\ 4) \\ g \downarrow & & \downarrow \downarrow \downarrow \downarrow \downarrow & & \text{where } g = (1\ 3\ 5\ 4). \\ y & = & (3\ 2\ 4)(5\ 1) \end{array} \quad (1)$$

That is, we replace the symbol 1 in x by the image of 1 under g , which is 3, and we replace the symbol 2 in x by the image of 2 under g , which is 2, and so on. The result is the permutation $y = (3\ 2\ 4)(5\ 1)$, as shown above. (Of course, after we have carried out these manipulations we could rewrite y in the usual way as $(1\ 5)(2\ 4\ 3)$, if we wished.)

To investigate the relationship between x , g and y , let us choose any symbol, say 4, and find the image of this symbol under the permutation y that results from the renaming. One way to find the image of 4 is simply to use the cycle form of y that was found above. This tells us that the image of 4 is 3, as illustrated below:

$$4 \xrightarrow{y} 3.$$

However, another way to find the image of 4 under y is to use the fact that y is just the permutation x with the symbols renamed, and use the cycle form of x to find the image. We proceed as follows. We first find the symbol that was renamed as 4. To do this, we need to go backwards along the arrow that points to the symbol 4 in diagram (1) above. That is, we need to find the image of 4 under the permutation g^{-1} . This gives the symbol 5. Then we use the cycle form of x to find the image of 5 under x . This gives 1. Finally, we find the symbol that is the new name of the symbol 1. That is, we find the image of 1 under the permutation g . This gives 3. So the image of 4 is 3. This process can be illustrated as follows.

$$\begin{array}{ccc} 5 & \xrightarrow{x} & 1 \\ g^{-1} \uparrow & & \downarrow g \\ 4 & & 3 \end{array}$$

As expected, this process gives the same final image, 3. Thus the effect of applying the permutation y to the symbol 4 is the same as the effect of applying the permutation g^{-1} , then the permutation x , then the permutation g , to the symbol 4. That is, the two permutations y and $g \circ x \circ g^{-1}$ have the same effect on the symbol 4. There is nothing special about the symbol 4 here, of course: the same will be true for any symbol in the set $\{1, 2, 3, 4, 5\}$. In other words, we can say that the two permutations y and $g \circ x \circ g^{-1}$ are equal.

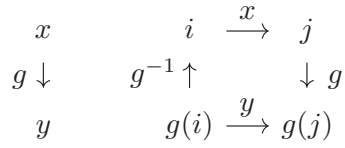


Figure 13 The effect of using a permutation g to rename the symbols in a permutation x to obtain a permutation y

The ideas above hold whenever we use a permutation g to rename the symbols in a permutation x to obtain another permutation y , as illustrated in Figure 13. In the figure, the symbol i is mapped to the symbol j by the permutation x , and the effect of the renaming is that the symbol $g(i)$ is mapped to the symbol $g(j)$ by the permutation y . By following the arrows in the figure, you can see that $g(i)$ is also mapped to $g(j)$ by the permutation $g \circ x \circ g^{-1}$. So, since $g(i)$ can be any symbol, the algebraic relationship between the three permutations x , g and y is

$$y = g \circ x \circ g^{-1}.$$

You may find this relationship rather surprising at first, but the next exercise should help to convince you that it is correct.

Exercise B114

This exercise is about permutations in S_5 . Let $x = (1\ 2\ 3\ 5)$.

- Let $g = (1\ 4)(2\ 5\ 3)$. Calculate $g \circ x \circ g^{-1}$ by finding g^{-1} and composing the three permutations. Compare your answer with the permutation obtained by using g to rename the symbols in x .
- Repeat part (a) for $g = (1\ 3\ 4\ 2\ 5)$.

Because of the algebraic relationship found above, we make the following definition.

Definitions

The permutation y is a **conjugate** of the permutation x in S_n if there is a permutation g in S_n such that

$$y = g \circ x \circ g^{-1}.$$

We say that:

- g **conjugates** x to y
- y is the **conjugate** of x by g
- g is a **conjugating permutation**.

Notice that the equation

$$y = g \circ x \circ g^{-1}$$

in the definition above can be rearranged as

$$g^{-1} \circ y \circ g = x$$

(by composing both sides of the original equation on the left by g^{-1} and on the right by g). The rearranged equation can be written as

$$x = g^{-1} \circ y \circ (g^{-1})^{-1}.$$

Thus if g conjugates x to y , then g^{-1} conjugates y to x . This makes sense, because if renaming the symbols in x using g gives y , then of course renaming the symbols in y using g^{-1} gives x . So if y is a conjugate of x , then x is a conjugate of y , and we say that x and y are **conjugates**, or **conjugate permutations**.

Since renaming the symbols in a permutation does not change its cycle structure, conjugate permutations always have the same cycle structure.



In fact, it is also true that any two permutations with the same cycle structure are conjugate permutations. This is because, given any two permutations x and y with the same cycle structure, we can always find a permutation g that conjugates x to y , as demonstrated in the next worked exercise.

Worked Exercise B44

Let $x = (1\ 2\ 4)(3\ 5)$ and $y = (1\ 4)(2\ 5\ 3)$ in S_5 .



- Find a permutation g in S_5 that conjugates x to y .
- Find two more permutations g in S_5 that conjugate x to y .

Solution

-  Write the cycle form of y underneath the cycle form of x , matching up cycles of the same length. Include any 1-cycles in the cycle forms if there are any – here there are none. 



We can write

$$\begin{array}{ccccccc} x & = & (1 & 2 & 4)(3 & 5) \\ g \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow \\ y & = & (2 & 5 & 3)(1 & 4). \end{array}$$

 This diagram is essentially the two-line form of a suitable conjugating permutation g . Write this permutation g in cycle form (using Strategy B7). 

A conjugating permutation g is

$$g = (1\ 2\ 5\ 4\ 3).$$

-  There are several alternative ways to match up the cycles in x and y , because the 3-cycle $(2\ 5\ 3)$ in y can alternatively be written as $(3\ 2\ 5)$ or $(5\ 3\ 2)$, and the 2-cycle $(1\ 4)$ in y can alternatively be written as $(4\ 1)$. 

Another conjugating permutation g is given by

$$\begin{array}{ccccccc} x & = & (1 & 2 & 4)(3 & 5) \\ g \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow \\ y & = & (3 & 2 & 5)(1 & 4). \end{array}$$

This gives $g = (1\ 3)(4\ 5)$.

A third conjugating permutation g is given by

$$\begin{array}{ccccccc} x & = & (1 & 2 & 4)(3 & 5) \\ g \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow & \\ y & = & (5 & 3 & 2)(4 & 1). \end{array}$$

This gives $g = (1 \ 5)(2 \ 3 \ 4)$.

Exercise B115

For the permutations x and y given in Worked Exercise B44, find three more permutations g in S_5 that conjugate x to y .

Here is a summary of the strategy used in Worked Exercise B44.

Strategy B12

To find a permutation g such that $y = g \circ x \circ g^{-1}$, where x and y are permutations with the same cycle structure, do the following.

Use the fact that g renames x to y , as follows.

1. Match up the cycles of x and y (including 1-cycles) so that cycles of equal lengths correspond.

$$\begin{array}{ccccccccccc} x & = & (*) & * & \cdots & *) & (*) & * & \cdots & *) & \cdots & (*) & (*) \\ g \downarrow & & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \cdots & \downarrow & \downarrow \\ y & = & (*) & * & \cdots & *) & (*) & * & \cdots & *) & \cdots & (*) & (*) \end{array}$$

2. Read off the two-line form of the renaming permutation g from this diagram. Usually, write g in cycle form.

Worked Exercise B44 and Exercise B115 illustrate the fact that if two permutations x and y are conjugate, then there can be many different permutations g that conjugate x to y .

You have now seen that if two permutations x and y have the same cycle structure, then it is always possible to find a permutation g that conjugates x to y , and hence x and y are conjugate. As mentioned earlier, it is also true that if two permutations are conjugate, then they have the same cycle structure (since renaming the symbols in a permutation does not change its cycle structure). Thus the following theorem holds.

Theorem B64

Two permutations in the symmetric group S_n are conjugate in S_n if and only if they have the same cycle structure.

Exercise B116

- (a) Find all permutations
- g
- in
- S_5
- such that

$$g \circ (1\ 2\ 3\ 4) \circ g^{-1} = (1\ 5\ 2\ 3).$$

- (b) Find all permutations
- g
- in
- S_4
- such that

$$g \circ (1\ 2)(3\ 4) \circ g^{-1} = (1\ 2)(3\ 4).$$

4.2 Conjugate subgroups in S_n

In this subsection we will return to looking at what happens when we use a permutation to rename the symbols in not just a single permutation, but in every permutation in a subgroup.

For example, consider again the subgroup of S_4 obtained by labelling the vertex locations of the square in the usual way, as shown in Figure 14. With this labelling, the set of symmetries of the square is represented by the following set of permutations in S_4 .

$$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), \\ (1\ 4)(2\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 3)\}$$

This set is a subgroup of S_4 , because it is a subset of S_4 and its elements represent all the symmetries of a figure.

At the start of the previous subsection we renamed the symbols in every permutation in this subgroup using the permutation $g = (2\ 3)$, which corresponds to relabelling the square as shown in Figure 15. We obtained the following set of permutations.

$$\{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3), \\ (1\ 4)(3\ 2), (3\ 4), (1\ 3)(2\ 4), (1\ 2)\}$$

This set is also a subgroup of S_4 , again because it is a subset of S_4 and its elements represent all the symmetries of a figure.

We will now look in general at what happens when we start with some subgroup of S_n , say H , and use a particular permutation g to rename the symbols in *all* the permutations in H .

As you saw in the previous subsection, when we rename the symbols in a single permutation x using a permutation g , the result is the conjugate permutation $g \circ x \circ g^{-1}$. In view of this, we use the following notation.

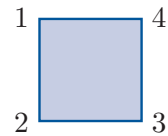


Figure 14 The square with its usual vertex labelling

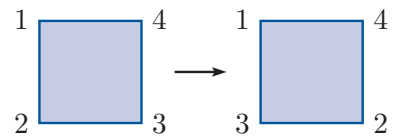


Figure 15 Relabelling the square using the permutation $g = (2\ 3)$

Notation

Let H be a subgroup of S_n , and let $g \in S_n$. Then we denote the set

$$\{g \circ h \circ g^{-1} : h \in H\}$$

by $g \circ H \circ g^{-1}$. That is, $g \circ H \circ g^{-1}$ is the set obtained by conjugating every element of H by the permutation g .

Thus if H is a subgroup of S_n , then $g \circ H \circ g^{-1}$ is the subset of S_n obtained by renaming the symbols in all the elements of H using g .

This definition is illustrated in the worked exercise below.



Worked Exercise B45

Let H be the cyclic subgroup of S_5 generated by the 4-cycle $(1\ 2\ 4\ 5)$; that is,

$$\begin{aligned} H &= \langle (1\ 2\ 4\ 5) \rangle \\ &= \{e, (1\ 2\ 4\ 5), (1\ 2\ 4\ 5)^2, (1\ 2\ 4\ 5)^3\} \\ &= \{e, (1\ 2\ 4\ 5), (1\ 4)(2\ 5), (1\ 5\ 4\ 2)\}. \end{aligned}$$

Find the set $g \circ H \circ g^{-1}$ where $g = (3\ 5)$.

Solution

 To conjugate each element of H by $g = (3\ 5)$, we rename the symbols in each element of H using this permutation. 

We have

$$g \circ H \circ g^{-1} = \{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}.$$

Notice that the set $g \circ H \circ g^{-1}$ found in Worked Exercise B45 is another subgroup of S_5 . You can see this because it is the cyclic subgroup generated by the 4-cycle $(1\ 2\ 4\ 3)$. (This 4-cycle is obtained by using g to rename the 4-cycle $(1\ 2\ 4\ 5)$ that generates the original subgroup H .)

In the next exercise you are asked to use a particular permutation g to rename the symbols in all the permutations in another cyclic subgroup of S_5 .

Exercise B117

Let H be the cyclic subgroup of S_5 generated by the 3-cycle $(1\ 3\ 5)$; that is,

$$\begin{aligned} H &= \langle (1\ 3\ 5) \rangle \\ &= \{e, (1\ 3\ 5), (1\ 3\ 5)^2\} \\ &= \{e, (1\ 3\ 5), (1\ 5\ 3)\}. \end{aligned}$$

- (a) Find the set $g \circ H \circ g^{-1}$ where $g = (1\ 4)(2\ 5)$.
 (b) Show that $g \circ H \circ g^{-1}$ is a subgroup of S_5 .

You have now seen several examples where we took a subgroup H of a symmetric group S_n , and renamed the symbols in all its elements using a permutation g in S_n . In each case the set $g \circ H \circ g^{-1}$ that we obtained was not just a *subset* of S_n but actually a *subgroup* of S_n . In fact, this is not surprising, as all we did in each case was to rename the symbols being permuted. The general result is stated below, with a proof that uses the formal definition of the set $g \circ H \circ g^{-1}$.

Theorem B65

Let H be a subgroup of S_n , and let $g \in S_n$. Then $g \circ H \circ g^{-1}$ is also a subgroup of S_n .

Proof We check the three subgroup properties.

SG1 Closure Consider any two elements of $g \circ H \circ g^{-1}$; we can write them as $g \circ h \circ g^{-1}$ and $g \circ k \circ g^{-1}$ where $h, k \in H$. We have

$$\begin{aligned} (g \circ h \circ g^{-1}) \circ (g \circ k \circ g^{-1}) &= g \circ h \circ (g^{-1} \circ g) \circ k \circ g^{-1} \\ &= g \circ h \circ e \circ k \circ g^{-1} \\ &= g \circ h \circ k \circ g^{-1}. \end{aligned}$$

This is an element of $g \circ H \circ g^{-1}$, because $h \circ k$ is an element of H (since H is a subgroup of S_n and therefore closed under \circ). Thus $g \circ H \circ g^{-1}$ is closed under \circ .

SG2 Identity The identity permutation e is in $g \circ H \circ g^{-1}$ since $e = g \circ e \circ g^{-1}$ and $e \in H$.

SG3 Inverses Consider any element of $g \circ H \circ g^{-1}$; we can write it as $g \circ h \circ g^{-1}$ where $h \in H$. We have

$$\begin{aligned} (g \circ h \circ g^{-1})^{-1} &= (g^{-1})^{-1} \circ h^{-1} \circ g^{-1} \\ &\quad \text{(by Proposition B14 in Unit B1, applied twice)} \\ &= g \circ h^{-1} \circ g^{-1} \quad \text{(by Proposition B13 in Unit B1).} \end{aligned}$$

This is an element of $g \circ H \circ g^{-1}$, because h^{-1} is an element of H (since H is a subgroup of S_n and therefore contains the inverse of each of its elements). Thus $g \circ H \circ g^{-1}$ contains the inverse of each of its elements.

Since $g \circ H \circ g^{-1}$ satisfies the three subgroup properties, it is a subgroup of S_n . ■

Because of Theorem B65, if H is a subgroup of S_n and g is an element of S_n , then we say that $g \circ H \circ g^{-1}$ is the **conjugate subgroup** of H by g , and that it is a **conjugate subgroup** of H in S_n .

When you are dealing with conjugate subgroups in S_n , keep in mind that if you want to find the elements of a conjugate subgroup $g \circ H \circ g^{-1}$, then you do not need to calculate composites of the form $g \circ h \circ g^{-1}$ by composing permutations. That would give you the right answer, but it would entail a lot of unnecessary calculation. Instead all you need to do is rename the symbols in each permutation h in H using g , as set out in the following strategy.

Strategy B13

To find the subgroup $g \circ H \circ g^{-1}$, given a subgroup H and an element g of S_n , do the following.

For each $h \in H$, find $g \circ h \circ g^{-1}$ by using g to ‘rename’ the symbols in h .

$$\begin{array}{ccccccc} h = & (* & * & \cdots & *) & (* & * & \cdots & *) & \cdots & (* & * & \cdots & *) \\ g \downarrow & & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow \\ g \circ h \circ g^{-1} = & (* & * & \cdots & *) & (* & * & \cdots & *) & \cdots & (* & * & \cdots & *) \end{array}$$

Exercise B118

Let H be the following subgroup of S_5 :

$$H = \{e, (1\ 2\ 5\ 3), (1\ 5)(2\ 3), (1\ 3\ 5\ 2)\}.$$

(H is the subgroup generated by the cycle $(1\ 2\ 5\ 3)$.)

Determine the following conjugate subgroups.

$$(a) \ (1\ 3) \circ H \circ (1\ 3)^{-1} \quad (b) \ (1\ 3)(2\ 4) \circ H \circ ((1\ 3)(2\ 4))^{-1}$$

Here are three more exercises that use the ideas that you have met in this subsection and the previous subsection.

Exercise B119

(a) Find all the permutations g in S_3 such that

$$g \circ (1\ 2\ 3) \circ g^{-1} = (1\ 2\ 3).$$

Show that they form a subgroup of S_3 .

(b) Find all the permutations g in S_4 such that

$$g \circ (1\ 2\ 3\ 4) \circ g^{-1} = (1\ 2\ 3\ 4).$$

Show that they form a subgroup of S_4 .

Exercise B120

Let (G, \circ) be a group and let f be a particular element of G . Prove that the set

$$C = \{g \in G : g \circ f \circ g^{-1} = f\}$$

is a subgroup of G .

(The facts that the two sets in Exercise B119 are subgroups of S_3 and S_4 , respectively, are special cases of this result.)

Exercise B121

Let H be the following subgroup of S_4 :

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

(We know that this subset of S_4 is a subgroup because its elements represent the symmetries of the rectangle, as you saw in Exercise B99.)

Prove that, for each element $g \in S_4$,

$$g \circ H \circ g^{-1} = H.$$

Having now reached the end of this section, you may be wondering why we have bothered with all the theory about the algebraic relationship $y = g \circ x \circ g^{-1}$, when it seems simpler just to use the idea of renaming the symbols in a permutation! However, the relationship $y = g \circ x \circ g^{-1}$ is helpful when we want to prove results involving conjugacy, because it can be used in algebraic manipulations. Also, expressing the idea of conjugacy in terms of this algebraic relationship rather than in terms of renaming symbols allows us to apply it to groups other than the symmetric groups S_n . This is a topic that you will learn much more about in Book E.

5 Subgroups of S_4

In this section we will find subgroups of S_4 , the symmetric group of degree 4, which is the group of all permutations of the set $\{1, 2, 3, 4\}$. We will start by finding all the cyclic subgroups of S_4 . Then we will find some non-cyclic subgroups. By the end of the section we will have found *all* the subgroups of S_4 , though we are not in a position to prove this fact at this stage. You should finish this section with some idea of the structure of S_4 .

Cyclic subgroups of S_4

In seeking the subgroups of any group, it is usually easiest to start with the cyclic subgroups. Remember that each element f of a group generates a cyclic subgroup $\langle f \rangle = \{e, f, f^2, \dots, f^{n-1}\}$ of order n , where n is the order of the element f . For example, the permutation $(1\ 2\ 3)$ in S_4 , which has order 3, generates the following cyclic subgroup of S_4 :

$$\begin{aligned}\langle (1\ 2\ 3) \rangle &= \{e, (1\ 2\ 3), (1\ 2\ 3)^2\} \\ &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}.\end{aligned}$$

It is important to remember that different elements of a group can generate the same cyclic subgroup. For example, the cyclic subgroup $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ of S_4 is also generated by the permutation $(1\ 3\ 2)$, since

$$\begin{aligned}\langle (1\ 3\ 2) \rangle &= \{e, (1\ 3\ 2), (1\ 3\ 2)^2\} \\ &= \{e, (1\ 3\ 2), (1\ 2\ 3)\}.\end{aligned}$$

In general, as you saw in Unit B2 *Groups and subgroups*, any element of order n in a cyclic subgroup of order n generates that subgroup.

A helpful first step towards finding all the cyclic subgroups of S_4 is to find the orders of all the elements of S_4 . You saw in Theorem B55 that the order of a permutation is the least common multiple of the lengths of its cycles. Table 3 gives the five different cycle structures in S_4 ; you were asked to find these in Exercise B92. For each cycle structure, the table also shows the order of the elements with that cycle structure, and lists those elements.

Table 3 The cycle structures and orders of the elements of S_4

Cycle structure	Order	Elements of S_4	Description
e	1	e	identity
$(--)$	2	$(1\ 2), (1\ 3), (1\ 4),$ $(2\ 3), (2\ 4), (3\ 4)$	transpositions
$(---)$	3	$(1\ 2\ 3), (1\ 3\ 2),$ $(1\ 2\ 4), (1\ 4\ 2),$ $(1\ 3\ 4), (1\ 4\ 3),$ $(2\ 3\ 4), (2\ 4\ 3)$	3-cycles
$(----)$	4	$(1\ 2\ 3\ 4), (1\ 2\ 4\ 3),$ $(1\ 3\ 2\ 4), (1\ 3\ 4\ 2),$ $(1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$	4-cycles
$(--)(--)$	2	$(1\ 2)(3\ 4),$ $(1\ 3)(2\ 4),$ $(1\ 4)(2\ 3)$	products of 2-cycles

From Table 3 we see that each element in S_4 has order 1, 2, 3 or 4, so each cyclic subgroup of S_4 has order 1, 2, 3 or 4.

Let us begin by finding the cyclic subgroups of order 3 (you are asked to find the cyclic subgroups of orders 1, 2 and 4 in the next exercise). In Subsection 4.4 of Unit B2 you saw that all cyclic groups of a particular order are isomorphic (structurally identical) to each other. They therefore contain the same number of elements of each order. In particular, each cyclic group of order 3 contains one element of order 1 (the identity) and two elements of order 3.

As shown in Table 3, the only elements of order 3 in S_4 are the 3-cycles. You saw above that the 3-cycles $(1\ 2\ 3)$ and $(1\ 3\ 2)$ each generate the subgroup $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$. The remaining six 3-cycles in S_4 ‘pair off’ in a similar way to generate the following cyclic subgroups:

$$\begin{aligned}\langle(1\ 4\ 2)\rangle &= \{e, (1\ 4\ 2), (1\ 2\ 4)\} = \langle(1\ 2\ 4)\rangle, \\ \langle(1\ 3\ 4)\rangle &= \{e, (1\ 3\ 4), (1\ 4\ 3)\} = \langle(1\ 4\ 3)\rangle, \\ \langle(2\ 3\ 4)\rangle &= \{e, (2\ 3\ 4), (2\ 4\ 3)\} = \langle(2\ 4\ 3)\rangle.\end{aligned}$$

So in total there are four cyclic subgroups of order 3. In the next exercise you are asked to find all the other cyclic subgroups of S_4 .

Exercise B122

Use Table 3 to help you do the following.

- Find all the cyclic subgroups of S_4 of orders 1, 2 and 4.
- Make a table showing the number of cyclic subgroups of S_4 of each possible order.

We have now found all the cyclic subgroups of S_4 .

Non-cyclic subgroups of S_4

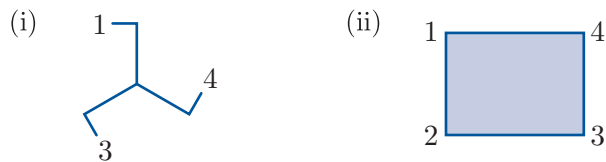
To find more subgroups of S_4 we need a method for finding non-cyclic subgroups.

We can use a method that you met in Subsection 2.4. To find a subgroup of any symmetric group S_n , we can draw a figure, labelled at suitable locations with some or all of the symbols $1, 2, \dots, n$, such that the symmetries of the figure can be represented by permutations of the labels. The symmetry group of the figure is then a subgroup of S_n . (Any symbols in $\{1, 2, \dots, n\}$ that are not used to label the figure are taken to be fixed.)

This method can yield both cyclic and non-cyclic subgroups, as illustrated for subgroups of S_4 in the next worked exercise.

Worked Exercise B46

Each of the two figures below is labelled with some or all of the symbols 1, 2, 3 and 4.



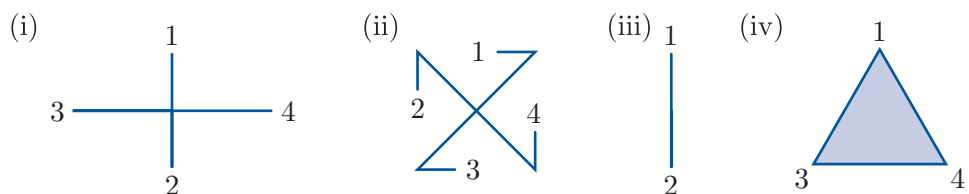
- (a) Use each figure to find a subgroup of S_4 .
- (b) State whether each of the subgroups in part (a) is cyclic, justifying your answers.

Solution

- (a) Using the labelling on the figures, we find that their symmetry groups can be represented by the following subgroups of S_4 .
- (i) $\{e, (1\ 3\ 4), (1\ 4\ 3)\}$
- (ii) $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
- (b) The subgroup in part (a)(i) is cyclic: it is generated by either of the 3-cycles that it contains. The subgroup in part (a)(ii) is non-cyclic, since it has order 4 but contains no element of order 4.

Exercise B123

- (a) Use the labelled figures below to find four subgroups of S_4 .

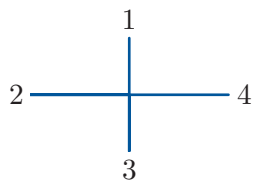


- (b) Which of the subgroups in part (a) are cyclic? Justify your answers.

Once we have found a subgroup of a symmetric group that is the symmetry group of a figure, we can often find another subgroup of the same symmetric group, isomorphic to the first subgroup, by relabelling the locations on the figure. Since the new subgroup is found from the old subgroup by relabelling in this way, it is *conjugate* to the first subgroup.

Exercise B124

- (a) The figure below is the same as the one in Exercise B123(a)(i), except that it has been relabelled. Use this figure to find a further subgroup of S_4 .



- (b) Find a third labelling of the same figure that yields a subgroup of S_4 different from the two subgroups found in part (a) and in Exercise B123(a)(i).

We have now found four different non-cyclic subgroups of S_4 of order 4, namely the one found in Worked Exercise B46, the one found in Exercise B123(a)(i) and the two found in Exercise B124. These are all isomorphic to the Klein four-group since, as you saw in Subsection 4.2 of Unit B2, the Klein four-group structure is the only possible structure for a non-cyclic group of order 4. Altogether we have now found seven subgroups of S_4 of order 4: the four non-cyclic ones, and the three cyclic ones from Exercise B122.

In the next two exercises you are asked to find subgroups of S_4 of orders 6 and 8, respectively.

Exercise B125

In Exercise B123(a)(iv) you found a subgroup of S_4 of order 6 that represents the symmetries of an equilateral triangle. By labelling the vertices of the triangle in three other ways, find three further subgroups of S_4 of order 6.

Exercise B126

- (a) Use a plane figure that has a symmetry group of order 8, with appropriate labels, to find a subgroup of S_4 of order 8.
- (b) By relabelling the figure in part (a) in two other ways, find two other subgroups of S_4 of order 8.

You have already met a subgroup of S_4 of order 12, namely A_4 , the subgroup of even permutations in S_4 . Taking this subgroup together with all the subgroups that we have found in this subsection so far, we now have all the subgroups of S_4 , although a proof that there are no more subgroups is beyond the scope of this module. Table 4 gives a summary of the number of subgroups of S_4 of each order.

Table 4 The subgroups of the symmetric group S_4

Order	Number of subgroups	Description
1	1	$\{e\}$
2	9	all cyclic
3	4	all cyclic
4	7	3 cyclic; 4 Klein
6	4	all isomorphic to $S(\triangle)$
8	3	all isomorphic to $S(\square)$
12	1	A_4
24	1	S_4

Exercise B127

- (a) Are all subgroups of order 2 conjugate to each other in S_4 ? Justify your answer.
- (b) Are all subgroups of order 3 conjugate to each other in S_4 ? Justify your answer.

You have now seen and used two methods that give subgroups of the group S_4 . A third simple way to find a subgroup of a symmetric group S_n is to find all the permutations in S_n that fix a particular symbol. For example, all the permutations in S_4 that fix the symbol 2 form a subgroup of S_4 . This is because the Cayley table for these permutations looks exactly the same as the group table for the group of all permutations of the set of symbols $\{1, 3, 4\}$ (provided that we use cycle form and omit 1-cycles).

In fact, the subgroup found in Exercise B123(a)(iv) is the set of all permutations in S_4 that fix the symbol 2, and the three subgroups found in Exercise B125 are the sets of all permutations in S_4 that fix the symbols 4, 3 and 1, respectively.

More generally, we can find a subgroup of a symmetric group S_n by finding all the permutations in S_n that fix each symbol in some subset of symbols; this follows from the same argument involving Cayley tables as used above. For example, $\{e, (1\ 2)\}$ is the subgroup of S_4 that consists of all permutations in S_4 that fix each element in the subset $\{3, 4\}$; its Cayley table looks exactly the same as the group table for the group of all permutations of the set of symbols $\{1, 2\}$.

Finding subgroups of groups in general

In this section you have seen three methods for finding subgroups of S_4 .

The first method, for finding cyclic subgroups, can be applied to any other group of reasonably small order. That is, you can find the cyclic subgroups of such a group by listing the elements of the group according to their orders and then systematically finding the subgroups generated by these elements.

The other two methods – namely, finding symmetry groups whose elements can be represented by permutations in S_4 , and finding all permutations that fix one or more symbols – are not useful for finding subgroups of groups in general, but can be used to find subgroups of any other *symmetric group* S_n . However, it is usually difficult to find *all* the non-cyclic subgroups of a symmetric group S_n using these methods.

To find subgroups of a *symmetry group*, both cyclic and non-cyclic, you can use the methods that you saw in Subsection 1.3 of Unit B2. For example, you can modify a figure to restrict its symmetry, or find the symmetries that fix a particular vertex of the figure.

S_4 as the symmetry group of a regular tetrahedron

The symmetric group S_4 can itself be thought of as a symmetry group, namely the symmetry group of a regular tetrahedron, $S(\text{tet})$. Remember from Unit B1 that there are 24 symmetries of the tetrahedron, and if the vertex locations are labelled 1, 2, 3 and 4 as shown in Figure 16, then each such symmetry can be represented by a permutation of the symbols 1, 2, 3 and 4; that is, as an element of S_4 . Moreover, since S_4 has order 24, every element of S_4 represents some symmetry of the tetrahedron. It follows that S_4 and $S(\text{tet})$ are isomorphic groups.

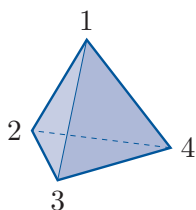


Figure 16 The regular tetrahedron

It can sometimes be enlightening to think of S_4 in this way. For example, it tells us that each of the subgroups of S_4 that we have found can be interpreted as a subgroup of $S(\text{tet})$.

For instance, with this interpretation, A_4 is the subgroup of direct symmetries of the tetrahedron. You can confirm this by checking that the twelve elements of A_4 , listed in Table 2 in Subsection 3.3, are the same permutations as the twelve direct symmetries of the tetrahedron with vertex locations labelled 1, 2, 3 and 4, found in Worked Exercise B14 in Subsection 5.3 of Unit B1. (Remember that for a bounded figure in \mathbb{R}^3 such as the tetrahedron, the direct symmetries are the rotational symmetries.)

In the next exercise you are asked to interpret some other subgroups of S_4 as subgroups of $S(\text{tet})$. It is interesting, but rather more difficult, to do this for some of the subgroups of S_4 other than the ones considered here.

Exercise B128

Describe in words each of the following subgroups of S_4 as subgroups of $S(\text{tet})$.

- (a) $\{e, (1\ 3\ 4), (1\ 4\ 3)\}$ (b) $\{e, (3\ 4)\}$
 (c) $\{e, (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}$ (d) $\{e, (1\ 2)(3\ 4)\}$

(The subgroup in part (c) was found in Exercise B125. The other three subgroups are cyclic subgroups.)

You saw earlier, in Subsection 2.4, that the symmetric group S_3 is also isomorphic to a symmetry group, namely $S(\triangle)$, the symmetry group of the equilateral triangle.

6 Cayley's Theorem

You have seen that the symmetry groups of many figures can be represented as permutation groups. What we mean by this is that these symmetry groups are *isomorphic* (structurally identical) to permutation groups. In this section you will see that, perhaps rather surprisingly, *every* finite group is isomorphic to a permutation group.

Remember from Unit B2 that for finite groups we can define the idea of isomorphism as follows: two finite groups are **isomorphic** if there is a one-to-one and onto mapping from the first group to the second group that transforms the group table of the first group into a group table for the second group. Such a mapping is called an **isomorphism**.

For example, consider the symmetry group of the rectangle. You have seen that when the vertices of the rectangle are labelled in the usual way, as shown in Figure 17, the symmetries of the rectangle can be represented as permutations as follows:

$$\begin{aligned} e, \\ a &= (1\ 3)(2\ 4), \\ r &= (1\ 4)(2\ 3), \\ s &= (1\ 2)(3\ 4). \end{aligned}$$

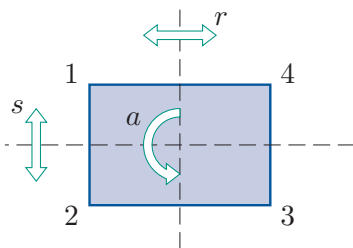


Figure 17 $S(\square)$

The symmetry group of the rectangle can then be represented by the permutation group (H, \circ) , where

$$H = \{e, (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}.$$

What we mean by this is that the two groups $(S(\square), \circ)$ and (H, \circ) are isomorphic, and the mapping

$$\begin{aligned}\phi: S(\square) &\longrightarrow H \\ e &\longmapsto e \\ a &\longmapsto (1\ 3)(2\ 4) \\ r &\longmapsto (1\ 4)(2\ 3) \\ s &\longmapsto (1\ 2)(3\ 4)\end{aligned}$$

is an isomorphism. It transforms the group table of $(S(\square), \circ)$ into a group table of (H, \circ) , as shown below.

\circ	e	a	r	s		\circ	e	$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$	$(1\ 2)(3\ 4)$
e	e	a	r	s		e	e	$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$	$(1\ 2)(3\ 4)$
a	a	e	s	r	\longrightarrow	$(1\ 3)(2\ 4)$	$(1\ 3)(2\ 4)$	e	$(1\ 2)(3\ 4)$	$(1\ 4)(2\ 3)$
r	r	s	e	a	ϕ	$(1\ 4)(2\ 3)$	$(1\ 4)(2\ 3)$	$(1\ 2)(3\ 4)$	e	$(1\ 3)(2\ 4)$
s	s	r	a	e		$(1\ 2)(3\ 4)$	$(1\ 2)(3\ 4)$	$(1\ 4)(2\ 3)$	$(1\ 3)(2\ 4)$	e
$(S(\square), \circ)$						(H, \circ)				

The way in which we represent the symmetry group of a figure as a permutation group is fairly intuitive: as you have seen, we label suitable locations on the figure and represent each symmetry of the figure by the corresponding permutation of the labels. It is much less obvious how we might go about representing other types of finite groups as permutation groups. However, it can be done: for example, here is how we can do it for the group $(\mathbb{Z}_6, +_6)$.

Representing the group $(\mathbb{Z}_6, +_6)$ as a permutation group

Consider the group table of $(\mathbb{Z}_6, +_6)$, as follows.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

With each element x of \mathbb{Z}_6 we associate the permutation p_x whose two-line form has as its first line the column headings of the group table and as its second line the row labelled x . For example, the element 2 of \mathbb{Z}_6 has associated permutation

$$p_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 0 & 1 \end{pmatrix}.$$

This gives us six permutations $p_0, p_1, p_2, p_3, p_4, p_5$, each permuting the set of symbols $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

We can write the six permutations $p_0, p_1, p_2, p_3, p_4, p_5$, in cycle form. For example, for the permutation p_2 , given above, we have

$$p_2 = (0\ 2\ 4)(1\ 3\ 5).$$

Doing this for all six permutations we obtain

$$p_0 = (0)(1)(2)(3)(4)(5) = e,$$

$$p_1 = (0\ 1\ 2\ 3\ 4\ 5),$$

$$p_2 = (0\ 2\ 4)(1\ 3\ 5),$$

$$p_3 = (0\ 3)(1\ 4)(2\ 5),$$

$$p_4 = (0\ 4\ 2)(1\ 5\ 3),$$

$$p_5 = (0\ 5\ 4\ 3\ 2\ 1).$$

Let us denote the set $\{p_0, p_1, p_2, p_3, p_4, p_5\}$ by P . Then P is a subset of the group of all permutations of the set of symbols $\{0, 1, 2, 3, 4, 5\}$.

We can construct a Cayley table for P by working out all the possible composites of two elements of P . For example,

$$p_1 \circ p_2 = (0\ 1\ 2\ 3\ 4\ 5) \circ (0\ 2\ 4)(1\ 3\ 5) = (0\ 3)(1\ 4)(2\ 5) = p_3.$$

If we do this, then we obtain the following Cayley table for (P, \circ) .

\circ	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_3	p_4	p_5	p_0
p_2	p_2	p_3	p_4	p_5	p_0	p_1
p_3	p_3	p_4	p_5	p_0	p_1	p_2
p_4	p_4	p_5	p_0	p_1	p_2	p_3
p_5	p_5	p_0	p_1	p_2	p_3	p_4

Notice that this Cayley table is exactly the same as the Cayley table for $(\mathbb{Z}_6, +_6)$, except that 0 has been replaced by p_0 , and 1 has been replaced by p_1 , and so on. In general, each element x of \mathbb{Z}_6 has been replaced by p_x . We know that the Cayley table for $(\mathbb{Z}_6, +_6)$ is a group table, so it follows that the Cayley table for (P, \circ) is also a group table (the two tables have exactly the same pattern: it is just that the symbols have different names). It also follows that the following mapping is an isomorphism:

$$\begin{aligned}\phi : \mathbb{Z}_6 &\longrightarrow P \\ x &\longmapsto p_x.\end{aligned}$$

So the group (P, \circ) is a representation of the group $(\mathbb{Z}_6, +_6)$ as a permutation group.

Representing any finite group as a permutation group

It turns out that we can use a method similar to that used above for $(\mathbb{Z}_6, +_6)$ to represent *any* finite group as a permutation group. That is, the theorem below holds. Here the symbol $*$ is used instead of our usual symbol \circ to denote the binary operation of a general group G , because the symbol \circ is needed to represent function composition, the binary operation of every permutation group.

Theorem B66

Let $(G, *)$ be a finite group. For each element x of G , let p_x be the permutation whose two-line form has as its first line the column headings of the group table of $(G, *)$ and as its second line the row labelled x in the group table. Let

$$P = \{p_x : x \in G\}.$$

Then (P, \circ) is a permutation group isomorphic to $(G, *)$.

Note that the two-line form for p_x described in Theorem B66 is definitely the two-line form of a *permutation*, as claimed in the statement of the theorem, because each element of G occurs exactly once in the column headings of the group table and, by Proposition B18 in Unit B1, each element of G also occurs exactly once in the row labelled x .

Notice also that the set of symbols being permuted by the permutations specified in Theorem B66 is the set G . So the symbols being permuted may not be numbers.

The following theorem follows immediately from Theorem B66: it is Theorem B66 without the details.

Theorem B67 Cayley's Theorem

Every finite group is isomorphic to a permutation group.

A proof of Theorem B66 (that is, essentially a proof of Cayley's Theorem) is provided at the end of this section for those who are interested.

Theorem B66 is illustrated in the next worked exercise and in the two exercises that follow it.

Worked Exercise B47

Construct a permutation group that is isomorphic to the group $(G, *)$ that has the following group table. Give the permutations in cycle form.

$*$	e	u	v	w	x	z
e	e	u	v	w	x	z
u	u	v	e	z	w	x
v	v	e	u	x	z	w
w	w	x	z	e	u	v
x	x	z	w	v	e	u
z	z	w	x	u	v	e

Solution

For each element of $(G, *)$, we find, in cycle form, the permutation whose two-line form has as its first line the column headings of the group table and as its second line the row of the group table labelled with that element.

$*$	e	u	v	w	x	z	
e	e	u	v	w	x	z	$\longrightarrow i$ (identity)
u	u	v	e	z	w	x	$\longrightarrow (e\ u\ v)(w\ z\ x)$
v	v	e	u	x	z	w	$\longrightarrow (e\ v\ u)(w\ x\ z)$
w	w	x	z	e	u	v	$\longrightarrow (e\ w)(u\ x)(v\ z)$
x	x	z	w	v	e	u	$\longrightarrow (e\ x)(u\ z)(v\ w)$
z	z	w	x	u	v	e	$\longrightarrow (e\ z)(u\ w)(v\ x)$

We do not use e to denote the identity permutation here, as e is already an element of the given group.

A permutation group that is isomorphic to the given group is

$$\{i, (e\ u\ v)(w\ z\ x), (e\ v\ u)(w\ x\ z), (e\ w)(u\ x)(v\ z), (e\ x)(u\ z)(v\ w), (e\ z)(u\ w)(v\ x)\},$$

where i is the identity permutation.

Exercise B129

Construct a permutation group that is isomorphic to the group that has the following group table. Give the permutations in cycle form.

\circ	e	a	b	c	p	q	r	s
e	e	a	b	c	p	q	r	s
a	a	e	c	b	q	p	s	r
b	b	c	a	e	r	s	q	p
c	c	b	e	a	s	r	p	q
p	p	q	s	r	a	e	b	c
q	q	p	r	s	e	a	c	b
r	r	s	p	q	c	b	a	e
s	s	r	q	p	b	c	e	a

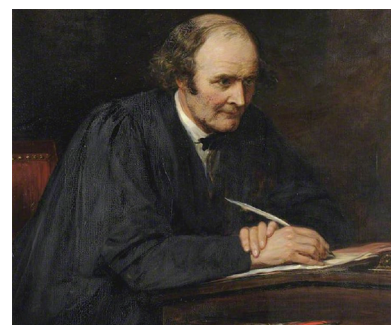
Exercise B130

Construct a permutation group that is isomorphic to the group (U_8, \times_8) , that is, $(\{1, 3, 5, 7\}, \times_8)$. Give the permutations in cycle form.

Cayley's Theorem (in its detailed form in Theorem B66), tells us that every finite group of order n is isomorphic to a subgroup of the symmetric group S_n . This is interesting because it suggests that to study finite groups it is sufficient to study only the symmetric groups and their subgroups. However, Cayley's Theorem is not very useful in practice; for example, to study groups of order 8 we would need to consider the subgroups of the symmetric group S_8 , which has order $8! = 40\,320$.

Cayley's Theorem can be generalised to infinite groups, but this is beyond the scope of this module.

Cayley's Theorem is named for the British mathematician Arthur Cayley (1821–1895) who in 1854 made the first advance towards the abstract notion of a finite group. Although he implicitly made the connection between group elements and permutations, he did not explicitly prove the theorem, which led to it later being ascribed to Jordan (who proved it in 1870). However, since Cayley communicated the result to the mathematical community at the time, credit for the theorem was soon restored to him.



Arthur Cayley

Proof of Cayley's Theorem (optional)

Here is a proof of Cayley's Theorem. It will not be assessed: read it if you are interested, and skip it if you are not.

To prove Cayley's Theorem we prove Theorem B66, which is as follows.

Theorem B66

Let $(G, *)$ be a finite group. For each element x of G , let p_x be the permutation whose two-line form has as its first line the column headings of the group table of $(G, *)$ and as its second line the row labelled x in the group table. Let

$$P = \{p_x : x \in G\}.$$

Then (P, \circ) is a permutation group isomorphic to $(G, *)$.

Proof Let $G = \{g_1, g_2, g_3, \dots, g_n\}$. For each element x of G , the row labelled x in the group table of G is as shown below.

*	g_1	g_2	g_3	\dots	g_n
g_1					
\vdots					
x	$x * g_1$	$x * g_2$	$x * g_3$	\dots	$x * g_n$
\vdots					
g_n					

Thus, for each element x of G , we have

$$p_x = \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ x * g_1 & x * g_2 & \dots & x * g_n \end{pmatrix}.$$

(As mentioned earlier, the two-line form here is definitely a *permutation*, because each element of G occurs exactly once in the column headings of the group table and exactly once in the row labelled x , by Proposition B18 in Unit B1.)

If x and y are different elements of G , then p_x and p_y are different permutations, since, for example, p_x maps the identity element of G to x whereas p_y maps it to y . Thus the set $P = \{p_x : x \in G\}$ contains the same number of elements as the original group G .

Now let p_x and p_y be any elements of P (not necessarily distinct). We will find a formula for their composite $p_x \circ p_y$ (that is, p_y followed by p_x). We have

$$p_x \circ p_y = \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ x * g_1 & x * g_2 & \dots & x * g_n \end{pmatrix} \circ \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ y * g_1 & y * g_2 & \dots & y * g_n \end{pmatrix}.$$

To compose the two two-line forms here, we start by finding the image of the symbol g_1 under $p_x \circ p_y$. First, p_y maps g_1 to $y * g_1$. The element $y * g_1$ of G appears somewhere in the top line of the two-line form of p_x and is mapped by p_x to $x * y * g_1$. So $p_x \circ p_y$ maps g_1 to $x * y * g_1$. Similarly, $p_x \circ p_y$ maps g_2 to $x * y * g_2$, and it maps g_3 to $x * y * g_3$, and so on. That is,

$$p_x \circ p_y = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ x * y * g_1 & x * y * g_2 & \cdots & x * y * g_n \end{pmatrix}.$$

But this is the two-line form of the permutation p_{x*y} associated with the element $x * y$ of G . Thus we have the formula

$$p_x \circ p_y = p_{x*y}.$$

We can use this formula to construct a Cayley table for the set P under function composition. It tells us that for each pair of permutations p_x and p_y in P , the entry in the row labelled p_x and column labelled p_y is p_{x*y} , as shown on the right below. We also know that in the Cayley table for the group $(G, *)$, the entry in the row labelled x and column labelled y is $x * y$, as shown on the left below.

$*$	\cdots	y	\cdots
\vdots		\vdots	
x	\cdots	$x * y$	\cdots
\vdots		\vdots	

$(G, *)$

\circ	\cdots	p_y	\cdots
\vdots		\vdots	
p_x	\cdots	p_{x*y}	\cdots
\vdots		\vdots	

(P, \circ)

So the Cayley table for the set P under function composition is exactly the same as the Cayley table of $(G, *)$, except that each element x of G has been replaced by the permutation p_x . We know that the Cayley table for $(G, *)$ is a group table, so it follows that the Cayley table for (P, \circ) is also a group table (the two tables have exactly the same pattern; it is just that the symbols have different names). It also follows that the two groups $(G, *)$ and (P, \circ) are isomorphic, and that the following mapping is an isomorphism:

$$\begin{aligned} \phi : G &\longrightarrow P \\ x &\longmapsto p_x. \end{aligned}$$

This completes the proof. ■

Summary

In this unit you have met the *symmetric groups*, each of which is a group whose elements are all the permutations of a set of symbols $\{1, 2, \dots, n\}$. The importance of these groups is highlighted by Cayley's Theorem, which states that every group is isomorphic to a subgroup of a symmetric group. You saw that we have been representing the symmetry groups of figures as subgroups of symmetric groups since early in Book B, even though we did not use the terms 'permutation' and 'symmetric group' until this unit. In this unit you have also met the idea of *conjugacy*. Symmetric groups provide a good illustration of this idea, and conjugacy in symmetric groups is important in its own right, but conjugacy is a powerful concept that can usefully be extended to all groups, as you will see in Book E.

Learning outcomes

After working through this unit, you should be able to:

- explain what is meant by a *permutation*
- convert a permutation from *two-line form* to *cycle form*
- find a *composite* of two or more permutations and the *inverse* of a permutation
- find the *order* of a permutation
- define the *symmetric group* S_n , and write down the elements of S_3 and S_4
- distinguish between *even* and *odd* permutations
- express a permutation as a composite of transpositions and understand the Parity Theorem
- define the *alternating group* A_n , and write down the elements of A_3 and A_4
- explain the meanings of the terms *conjugate elements* and *conjugate subgroups* in the context of the group S_n
- given any two permutations x and y in S_n with the same cycle structure, find all permutations in S_n that conjugate x to y
- determine subgroups of S_n that are conjugate to a given subgroup
- find all the cyclic subgroups of a particular order in a small symmetric group S_n , given all the elements of that order
- find some non-cyclic subgroups of a symmetric group S_n by finding symmetry groups whose elements can be represented by permutations in S_n
- know Cayley's Theorem
- represent a small finite group as a permutation group by using its group table.

Solutions to exercises

Solution to Exercise B81

(a) We trace the images of the symbols in the order in which they are encountered, starting at the symbol 1.

(i) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

we get

$$1 \longrightarrow 3 \longrightarrow 4 \longrightarrow 2 \longrightarrow 1,$$

so the cycle form is

$$(1\ 3\ 4\ 2).$$

(ii) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 6 & 2 & 1 & 4 \end{pmatrix}$$

we get

$$1 \longrightarrow 5 \longrightarrow 2 \longrightarrow 3 \longrightarrow 7 \longrightarrow 4 \longrightarrow 6 \longrightarrow 1,$$

so the cycle form is

$$(1\ 5\ 2\ 3\ 7\ 4\ 6).$$

(b) Here we carry out the process in part (a) in reverse.

(i) For the cycle $(1\ 3\ 2)$, we get

$$1 \mapsto 3, \quad 3 \mapsto 2, \quad 2 \mapsto 1,$$

so the two-line form is

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

(ii) For the cycle $(1\ 6\ 2\ 4\ 3\ 5)$ we get

$$\begin{aligned} 1 \mapsto 6, \quad 6 \mapsto 2, \quad 2 \mapsto 4, \quad 4 \mapsto 3, \\ 3 \mapsto 5, \quad 5 \mapsto 1, \end{aligned}$$

so the two-line form is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

(c) Starting at the symbol 1 (or 4, 3, 8 or 5) and following the same procedure as in part (a) we get the cycle $(1\ 4\ 3\ 8\ 5)$, which completes after only five symbols. Had we started at the symbol 2, 6 or 7, we would have obtained the cycle $(2\ 6)$ or (7) . So, no matter which symbol we start at, we cannot find a single cycle that contains all eight symbols.

Solution to Exercise B82

(a) Starting the cycle $(1\ 4\ 3\ 8\ 5)$ at 8 we get $(8\ 5\ 1\ 4\ 3)$, and $(2\ 6)$ is the same as $(6\ 2)$, so the cycle form of g may be written as

$$(7)(8\ 5\ 1\ 4\ 3)(6\ 2).$$

(b) Similarly, starting the cycle $(1\ 4\ 3\ 8\ 5)$ at 5 we get $(5\ 1\ 4\ 3\ 8)$, so the cycle form of g may be written as

$$(5\ 1\ 4\ 3\ 8)(2\ 6)(7).$$

Solution to Exercise B83

(The solution to this exercise contains the details of the process of obtaining the answers, but you need only give the final answers.)

(a) We trace the images of the symbols in the order in which they are encountered, starting at the symbol 1.

(i) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 1 & 5 & 3 \end{pmatrix},$$

we get

$$1 \longrightarrow 2 \longrightarrow 6 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1;$$

that is, the cycle $(1\ 2\ 6\ 3\ 4)$.

The remaining symbol 5 is mapped to itself. So the cycle form of this permutation is

$$(1\ 2\ 6\ 3\ 4)(5).$$

(ii) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 9 & 1 & 3 & 8 & 2 & 6 & 4 \end{pmatrix},$$

we get

$$1 \longrightarrow 5 \longrightarrow 3 \longrightarrow 9 \longrightarrow 4 \longrightarrow 1;$$

that is, the cycle $(1\ 5\ 3\ 9\ 4)$.

The symbol 2 has not yet been placed in a cycle. Starting at 2 we get

$$2 \longrightarrow 7 \longrightarrow 2;$$

that is, the cycle $(2\ 7)$.

The symbol 6 has not yet been placed in a cycle. Starting at 6 we get

$$6 \longrightarrow 8 \longrightarrow 6;$$

that is, the cycle (6 8).

All the symbols have now been placed in cycles, so the cycle form of this permutation is

$$(1\ 5\ 3\ 9\ 4)(2\ 7)(6\ 8).$$

(b) (i) For the permutation (1 6)(2 3 7 5)(4), the cycle form tells us that

$$\begin{aligned} 1 &\mapsto 6, & 6 &\mapsto 1; \\ 2 &\mapsto 3, & 3 &\mapsto 7, & 7 &\mapsto 5, & 5 &\mapsto 2; \\ 4 &\mapsto 4. \end{aligned}$$

We have now found the image of each symbol, so the two-line form for this permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 7 & 4 & 2 & 1 & 5 \end{pmatrix}.$$

(ii) For the permutation (1 6 4 2)(3 5 8)(7), the cycle form tells us that

$$\begin{aligned} 1 &\mapsto 6, & 6 &\mapsto 4, & 4 &\mapsto 2, & 2 &\mapsto 1; \\ 3 &\mapsto 5, & 5 &\mapsto 8, & 8 &\mapsto 3; \\ 7 &\mapsto 7. \end{aligned}$$

We have now found the image of each symbol, so the two-line form for this permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 5 & 2 & 8 & 4 & 7 & 3 \end{pmatrix}.$$

Solution to Exercise B84

The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 4 & 8 & 3 & 6 & 1 & 5 \end{pmatrix}$$

has cycle form

$$(1\ 7)(2)(3\ 4\ 8\ 5)(6),$$

that is,

$$(1\ 7)(3\ 4\ 8\ 5).$$

Solution to Exercise B85

We follow the convention of assuming that symbols in the set $\{1, 2, 3, 4, 5\}$ that are omitted from a cycle form are fixed by the permutation.

(a) The two-line form of the permutation (1 4)(2 5) is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

(b) The two-line form of the permutation (1 2) is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}.$$

(c) The two-line form of the permutation (1 5 4) is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

(d) The two-line form of the permutation e is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Solution to Exercise B86

(The solution to this exercise contains the details of the process of obtaining the answers, but you need only give the final answers.)

We use Strategy B8. In each case we start with the symbol 1 and find the cycle containing 1.

As in Worked Exercise B33, the set of symbols is $\{1, 2, 3, 4, 5, 6\}$, and

$$f = (1\ 4\ 3)(2\ 6), \text{ so } f \text{ fixes } 5,$$

$$g = (1\ 4\ 6\ 2\ 5), \text{ so } g \text{ fixes } 3.$$

(a) Remember that $f \circ g$ means ‘ g first, then f ’, so

$$(f \circ g)(x) = f(g(x)).$$

For the composite $f \circ g$ we have

$$1 \xrightarrow{g} 4 \text{ and } 4 \xrightarrow{f} 3, \text{ so } 1 \xrightarrow{f \circ g} 3,$$

$$3 \xrightarrow{g} 3 \text{ and } 3 \xrightarrow{f} 1, \text{ so } 3 \xrightarrow{f \circ g} 1.$$

So the composite contains the cycle (1 3).

Next we consider the symbol 2:

$$2 \xrightarrow{g} 5 \text{ and } 5 \xrightarrow{f} 5, \text{ so } 2 \xrightarrow{f \circ g} 5,$$

$$5 \xrightarrow{g} 1 \text{ and } 1 \xrightarrow{f} 4, \text{ so } 5 \xrightarrow{f \circ g} 4,$$

$$4 \xrightarrow{g} 6 \text{ and } 6 \xrightarrow{f} 2, \text{ so } 4 \xrightarrow{f \circ g} 2.$$

So the composite contains the cycle (2 5 4).

Finally,

$$6 \xrightarrow{g} 2 \text{ and } 2 \xrightarrow{f} 6, \text{ so } 6 \xrightarrow{f \circ g} 6.$$

Thus, omitting the 1-cycle (6), we have

$$f \circ g = (1\ 3)(2\ 5\ 4).$$

(b) For the composite $f \circ f$ we have

$$1 \xrightarrow{f} 4 \text{ and } 4 \xrightarrow{f} 3, \text{ so } 1 \xrightarrow{f \circ f} 3,$$

$$3 \xrightarrow{f} 1 \text{ and } 1 \xrightarrow{f} 4, \text{ so } 3 \xrightarrow{f \circ f} 4,$$

$$4 \xrightarrow{f} 3 \text{ and } 3 \xrightarrow{f} 1, \text{ so } 4 \xrightarrow{f \circ f} 1.$$

So the composite contains the cycle (1 3 4).

The permutation f contains the cycle (2 6), so $f \circ f$ fixes both 2 and 6 (since it interchanges them twice).

Finally, f fixes 5, so $f \circ f$ also fixes 5.

Thus

$$f \circ f = (1\ 3\ 4).$$

(c) For the composite $g \circ g$ we have

$$1 \xrightarrow{g} 4 \text{ and } 4 \xrightarrow{g} 6, \text{ so } 1 \xrightarrow{g \circ g} 6,$$

$$6 \xrightarrow{g} 2 \text{ and } 2 \xrightarrow{g} 5, \text{ so } 6 \xrightarrow{g \circ g} 5,$$

$$5 \xrightarrow{g} 1 \text{ and } 1 \xrightarrow{g} 4, \text{ so } 5 \xrightarrow{g \circ g} 4,$$

$$4 \xrightarrow{g} 6 \text{ and } 6 \xrightarrow{g} 2, \text{ so } 4 \xrightarrow{g \circ g} 2,$$

$$2 \xrightarrow{g} 5 \text{ and } 5 \xrightarrow{g} 1, \text{ so } 2 \xrightarrow{g \circ g} 1.$$

So the composite contains the cycle (1 6 5 4 2).

Finally, g fixes 3, so $g \circ g$ also fixes 3.

Thus

$$g \circ g = (1\ 6\ 5\ 4\ 2).$$

Solution to Exercise B87

We use Strategy B8. Notice that the set is $\{1, 2, 3, 4, 5, 6\}$, and

$$f = (1\ 3\ 2\ 4\ 6), \text{ so } f \text{ fixes } 5,$$

$$g = (1\ 4)(3\ 5), \text{ so } g \text{ fixes } 2 \text{ and } 6.$$

$$\begin{aligned} \text{(a)} \quad g \circ f &= (1\ 4)(3\ 5) \circ (1\ 3\ 2\ 4\ 6) \\ &= (1\ 5\ 3\ 2)(4\ 6). \end{aligned}$$

$$\begin{aligned} \text{(b)} \quad f \circ g &= (1\ 3\ 2\ 4\ 6) \circ (1\ 4)(3\ 5) \\ &= (1\ 6)(2\ 4\ 3\ 5). \end{aligned}$$

$$\begin{aligned} \text{(c)} \quad f \circ f &= (1\ 3\ 2\ 4\ 6) \circ (1\ 3\ 2\ 4\ 6) \\ &= (1\ 2\ 6\ 3\ 4). \end{aligned}$$

(d) The permutation g consists of cycles each of which interchanges two symbols. Performing such a cycle twice interchanges the two symbols twice, so $g \circ g = e$.

Solution to Exercise B88

We use Strategy B8, adapted to apply to three or more permutations.

(a) We have

$$\begin{aligned} &(1\ 3)(2\ 4)(5\ 7\ 6) \circ (1\ 7\ 6)(2\ 3) \circ (1\ 7\ 4\ 6) \\ &= (1\ 5\ 7\ 2)(3\ 4)(6) = (1\ 5\ 7\ 2)(3\ 4). \end{aligned}$$

(b) Here

$$\begin{aligned} &(1\ 7\ 3\ 4\ 6) \circ (1\ 2) \circ (3\ 7) \circ (5\ 3) \\ &= (1\ 2\ 7\ 4\ 6)(3\ 5). \end{aligned}$$

Solution to Exercise B89

Following Strategy B9 we obtain the inverse by writing each cycle in reverse order.

$$\begin{aligned} \text{(a)} \quad (1\ 6\ 4\ 2\ 5\ 8\ 3\ 7)^{-1} &= (7\ 3\ 8\ 5\ 2\ 4\ 6\ 1) \\ &= (1\ 7\ 3\ 8\ 5\ 2\ 4\ 6) \end{aligned}$$

$$\begin{aligned} \text{(b)} \quad ((1\ 5\ 4\ 7)(2\ 6\ 8))^{-1} &= (7\ 4\ 5\ 1)(8\ 6\ 2) \\ &= (1\ 7\ 4\ 5)(2\ 8\ 6) \end{aligned}$$

$$\begin{aligned} \text{(c)} \quad ((1\ 8)(2\ 7)(3\ 5))^{-1} &= (8\ 1)(7\ 2)(5\ 3) \\ &= (1\ 8)(2\ 7)(3\ 5). \end{aligned}$$

Notice that the permutation (1 8)(2 7)(3 5) is its own inverse. This is because each of its cycles interchanges two symbols.

Solution to Exercise B90

(a) In part (i) we use Strategy B8 and in parts (ii)–(iv) we use Strategy B9.

$$\text{(i)} \quad g \circ f = (1\ 5\ 3\ 6\ 2)$$

$$\begin{aligned} \text{(ii)} \quad f^{-1} &= (5\ 4\ 6\ 2\ 1) \\ &= (1\ 5\ 4\ 6\ 2) \end{aligned}$$

$$\begin{aligned} \text{(iii)} \quad g^{-1} &= (6\ 3\ 1)(4\ 5\ 2) \\ &= (1\ 6\ 3)(2\ 4\ 5) \end{aligned}$$

$$\begin{aligned} \text{(iv)} \quad (g \circ f)^{-1} &= (1\ 5\ 3\ 6\ 2)^{-1} = (2\ 6\ 3\ 5\ 1) \\ &= (1\ 2\ 6\ 3\ 5) \end{aligned}$$

(b) Strategy B8 gives

$$\begin{aligned} f^{-1} \circ g^{-1} &= (1\ 5\ 4\ 6\ 2) \circ (1\ 6\ 3)(2\ 4\ 5) \\ &= (1\ 2\ 6\ 3\ 5), \end{aligned}$$

which is the expression for $(g \circ f)^{-1}$ that was found in part (a)(iv).

(Remember that the equation

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

holds for any two one-to-one functions f and g , as mentioned immediately after the proof of Proposition B14 in Unit B1.)

Solution to Exercise B91

(a) In two-line form, the elements of S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

In cycle form, they are

$$e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2).$$

Thus S_3 has order 6.

(b) We count how many different ways there are to complete the bottom row of the two-line form of a permutation of the set $\{1, 2, 3, 4\}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}.$$

There are 4 choices for the symbol to be placed in the first position in the bottom row.

Once we have chosen this symbol, there are only 3 symbols still to be placed, so there are 3 choices for the symbol to be placed in the second position.

Once we have chosen the first two symbols, there are only 2 symbols still to be placed, so there are 2 choices for the symbol to be placed in the third position.

Finally, there is just 1 choice left for the symbol to be placed in the fourth position.

The total number of ways to complete the bottom row is therefore

$$4 \times 3 \times 2 \times 1 = 4! = 24.$$

That is, the group S_4 has order 24.

(The number of ways to fill in the bottom row is the number of permutations of 4 symbols from 4, in the sense in which the word ‘permutation’ is used in combinatorics. You may know that this is written as 4P_4 , and is equal to $4! = 24$.)

Solution to Exercise B92

There are five possible cycle structures in S_4 . A representative permutation for each cycle structure is given in the following table.

Cycle structure	Element of S_4	Description
e	e	identity
$(- \ -)$	$(1\ 2)$	transposition
$(- \ - \ -)$	$(1\ 2\ 3)$	3-cycle
$(- \ - \ - \ -)$	$(1\ 2\ 3\ 4)$	4-cycle
$(- \ -)(- \ -)$	$(1\ 2)(3\ 4)$	two 2-cycles

Solution to Exercise B93

There are seven possible cycle structures in S_5 . A representative permutation for each cycle structure is given in the following table.

Cycle structure	Element of S_5	Description
e	e	identity
$(- \ -)$	$(1\ 2)$	transposition
$(- \ - \ -)$	$(1\ 2\ 3)$	3-cycle
$(- \ - \ - \ -)$	$(1\ 2\ 3\ 4)$	4-cycle
$(- \ - \ - \ - \ -)$	$(1\ 2\ 3\ 4\ 5)$	5-cycle
$(- \ -)(- \ -)$	$(1\ 2)(3\ 4)$	two 2-cycles
$(- \ -)(- \ - \ -)$	$(1\ 2)(3\ 4\ 5)$	2-cycle and 3-cycle

Solution to Exercise B94

For the permutation $f = (1\ 6\ 3\ 7\ 5\ 2)$,

$$f^2 = (1\ 3\ 5)(2\ 6\ 7),$$

$$f^3 = (1\ 7)(2\ 3)(5\ 6),$$

$$f^4 = (1\ 5\ 3)(2\ 7\ 6),$$

$$f^5 = (1\ 2\ 5\ 7\ 3\ 6),$$

$$f^6 = e.$$

So the 6-cycle f has order 6.

Solution to Exercise B95

By Theorem B55, the order of a permutation is the least common multiple of the lengths of its cycles.

(a) The cycle lengths are 4, 2 and 2, so the order is 4.

(b) The cycle lengths are 3 and 5, so the order is 15.

(c) The cycle lengths are 2, 2, 2 and 3, so the order is 6.

(d) The cycle lengths are 3 and 3, so the order is 3.

Solution to Exercise B96

(a) The permutation $(1\ 5\ 2\ 3)$ has order 4, so

$$\begin{aligned} \langle (1\ 5\ 2\ 3) \rangle &= \{e, (1\ 5\ 2\ 3), (1\ 5\ 2\ 3)^2, (1\ 5\ 2\ 3)^3\} \\ &= \{e, (1\ 5\ 2\ 3), (1\ 2)(3\ 5), (1\ 3\ 2\ 5)\}. \end{aligned}$$

(b) The permutation $(1\ 4\ 2)(3\ 5)$ has order 6, so

$$\begin{aligned} \langle (1\ 4\ 2)(3\ 5) \rangle &= \{e, (1\ 4\ 2)(3\ 5), ((1\ 4\ 2)(3\ 5))^2, \\ &\quad ((1\ 4\ 2)(3\ 5))^3, ((1\ 4\ 2)(3\ 5))^4, \\ &\quad ((1\ 4\ 2)(3\ 5))^5\} \\ &= \{e, (1\ 4\ 2)(3\ 5), (1\ 2\ 4), (3\ 5), (1\ 4\ 2), \\ &\quad (1\ 2\ 4)(3\ 5)\}. \end{aligned}$$

Solution to Exercise B97

The set S is a subset of S_6 , since its elements permute the symbols 1, 2, 3, 4, 5 and 6 (fixing 2, 3 and 4). Also, the permutation $(1\ 5\ 6)$ has order 3, so

$$\begin{aligned} \langle (1\ 5\ 6) \rangle &= \{e, (1\ 5\ 6), (1\ 5\ 6)^2\} \\ &= \{e, (1\ 5\ 6), (1\ 6\ 5)\} \\ &= S. \end{aligned}$$

Hence S is the cyclic subgroup of S_6 generated by $(1\ 5\ 6)$; in particular, it is a subgroup of S_6 .

Solution to Exercise B98

The symmetries in $S(\triangle)$ and their orders are shown below.

	Symmetry	Order
Rotations	e	1
	$a = (1\ 2\ 3)$	3
	$b = (1\ 3\ 2)$	3
Reflections	$r = (2\ 3)$	2
	$s = (1\ 3)$	2
	$t = (1\ 2)$	2

Solution to Exercise B99

The symmetries in $S(\square)$ and their orders are shown below.

	Symmetry	Order
Rotations	e	1
	$a = (1\ 3)(2\ 4)$	2
Reflections	$r = (1\ 4)(2\ 3)$	2
	$s = (1\ 2)(3\ 4)$	2

Solution to Exercise B100

The symmetries of the hexagon and their orders are shown below.

	Symmetry	Order
Rotations	e	1
	$(1\ 2\ 3\ 4\ 5\ 6)$	6
	$(1\ 3\ 5)(2\ 4\ 6)$	3
	$(1\ 4)(2\ 5)(3\ 6)$	2
	$(1\ 5\ 3)(2\ 6\ 4)$	3
	$(1\ 6\ 5\ 4\ 3\ 2)$	6
Reflections	$(1\ 6)(2\ 5)(3\ 4)$	2
	$(1\ 2)(3\ 6)(4\ 5)$	2
	$(1\ 4)(2\ 3)(5\ 6)$	2
	$(2\ 6)(3\ 5)$	2
	$(1\ 3)(4\ 6)$	2
	$(1\ 5)(2\ 4)$	2

Solution to Exercise B101

The symmetries of the figure are represented by the following permutations in S_3 :

$$e, (1\ 2\ 3), (1\ 3\ 2).$$

(Since the symmetries form a group, these three symmetries form a subgroup of S_3 .)

Solution to Exercise B102

A subgroup of S_5 is

$$\{e, (1\ 4)(2\ 5), (1\ 5)(2\ 4), (1\ 2)(4\ 5)\}.$$

Solution to Exercise B103

The identity symmetry e fixes all four edges.

The rotation through a half turn transposes opposite pairs of edges, namely 1, 2 and 3, 4, so

$$a = (1\ 2)(3\ 4).$$

Reflection in the vertical axis of symmetry maps the edges 1 and 2 to themselves and transposes the edges 3 and 4, so

$$r = (3\ 4).$$

Reflection in the horizontal axis of symmetry maps the edges 3 and 4 to themselves and transposes the edges 1 and 2, so

$$s = (1\ 2).$$

So, with this labelling of the rectangle, the symmetry group is

$$\{e, (1\ 2)(3\ 4), (3\ 4), (1\ 2)\}.$$

Solution to Exercise B104

The symmetries of the double tetrahedron are represented by the following permutations in S_6 .

e	$(1\ 4)(2\ 5)(3\ 6)$
$(1\ 2\ 3)(4\ 5\ 6)$	$(1\ 5\ 3\ 4\ 2\ 6)$
$(1\ 3\ 2)(4\ 6\ 5)$	$(1\ 6\ 2\ 4\ 3\ 5)$
$(1\ 2)(4\ 5)$	$(1\ 5)(2\ 4)(3\ 6)$
$(1\ 3)(4\ 6)$	$(1\ 6)(2\ 5)(3\ 4)$
$(2\ 3)(5\ 6)$	$(1\ 4)(2\ 6)(3\ 5)$

(The permutations in the first column are the symmetries obtained from the symmetries of the

equilateral triangle in the middle of the double tetrahedron. The first symmetry in the second column is the reflection in the horizontal plane through the middle of the double tetrahedron. The remaining symmetries in the second column are obtained by composing each of the permutations in the first column with the first permutation in the second column, in that order.)

Solution to Exercise B105

(a) (*The solution to this exercise contains the details of the process of obtaining the answers, but you need only give the final answers.*)

In each case we find the image of each symbol in turn, starting with the symbol 1.

(i) For the composite $(1\ 4) \circ (1\ 2)$ we have

$$1 \mapsto 2, \text{ then } 2 \mapsto 2, \text{ so } 1 \mapsto 2;$$

$$2 \mapsto 1, \text{ then } 1 \mapsto 4, \text{ so } 2 \mapsto 4;$$

$$4 \mapsto 4, \text{ then } 4 \mapsto 1, \text{ so } 4 \mapsto 1.$$

Thus

$$(1\ 4) \circ (1\ 2) = (1\ 2\ 4).$$

(ii) For the composite $(1\ 3) \circ (1\ 2) \circ (1\ 4)$ we have

$$1 \mapsto 4, \text{ then } 4 \mapsto 4, \text{ then } 4 \mapsto 4, \text{ so } 1 \mapsto 4;$$

$$4 \mapsto 1, \text{ then } 1 \mapsto 2, \text{ then } 2 \mapsto 2, \text{ so } 4 \mapsto 2;$$

$$2 \mapsto 2, \text{ then } 2 \mapsto 1, \text{ then } 1 \mapsto 3, \text{ so } 2 \mapsto 3;$$

$$3 \mapsto 3, \text{ then } 3 \mapsto 3, \text{ then } 3 \mapsto 1, \text{ so } 3 \mapsto 1.$$

Thus

$$(1\ 3) \circ (1\ 2) \circ (1\ 4) = (1\ 4\ 2\ 3).$$

(iii) For the composite $(3\ 1) \circ (3\ 4) \circ (3\ 2)$ we have

$$1 \mapsto 1, \text{ then } 1 \mapsto 1, \text{ then } 1 \mapsto 3, \text{ so } 1 \mapsto 3;$$

$$3 \mapsto 2, \text{ then } 2 \mapsto 2, \text{ then } 2 \mapsto 2, \text{ so } 3 \mapsto 2;$$

$$2 \mapsto 3, \text{ then } 3 \mapsto 4, \text{ then } 4 \mapsto 4, \text{ so } 2 \mapsto 4;$$

$$4 \mapsto 4, \text{ then } 4 \mapsto 3, \text{ then } 3 \mapsto 1, \text{ so } 4 \mapsto 1.$$

Thus

$$(3\ 1) \circ (3\ 4) \circ (3\ 2) = (1\ 3\ 2\ 4).$$

(b) In part (a) we found that

$$(1\ 4) \circ (1\ 2) = (1\ 2\ 4),$$

$$(1\ 3) \circ (1\ 2) \circ (1\ 4) = (1\ 4\ 2\ 3),$$

$$(3\ 1) \circ (3\ 4) \circ (3\ 2) = (3\ 2\ 4\ 1).$$

(The last cycle has been reordered to make the pattern obvious.)

In each case the composite is a cycle in which the symbol common to all the transpositions is followed by the other symbols from the transpositions *in their order of appearance from right to left*.

Using this pattern we obtain the following, which can be checked by composing the transpositions:

$$(1 \ 4 \ 3) = (1 \ 3) \circ (1 \ 4),$$

$$(1 \ 4 \ 3 \ 2) = (1 \ 2) \circ (1 \ 3) \circ (1 \ 4).$$

Solution to Exercise B106

Following Strategy B10 we obtain the following.

$$(a) \ (1 \ 5 \ 2 \ 7 \ 3) = (1 \ 3) \circ (1 \ 7) \circ (1 \ 2) \circ (1 \ 5)$$

$$(b) \ (2 \ 3 \ 7 \ 5 \ 4 \ 6) = (2 \ 6) \circ (2 \ 4) \circ (2 \ 5) \circ (2 \ 7) \circ (2 \ 3)$$

$$(c) \ (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7) \\ = (1 \ 7) \circ (1 \ 6) \circ (1 \ 5) \circ (1 \ 4) \circ (1 \ 3) \circ (1 \ 2)$$

Solution to Exercise B107

(a) A 4-cycle is a composite of three transpositions:

$$(a_1 \ a_2 \ a_3 \ a_4) = (a_1 \ a_4) \circ (a_1 \ a_3) \circ (a_1 \ a_2).$$

(b) A 5-cycle is a composite of four transpositions:

$$(a_1 \ a_2 \ a_3 \ a_4 \ a_5) \\ = (a_1 \ a_5) \circ (a_1 \ a_4) \circ (a_1 \ a_3) \circ (a_1 \ a_2).$$

(c) An r -cycle is a composite of $r - 1$ transpositions:

$$(a_1 \ a_2 \ \dots \ a_{r-1} \ a_r) \\ = (a_1 \ a_r) \circ (a_1 \ a_{r-1}) \circ \dots \circ (a_1 \ a_2).$$

Solution to Exercise B108

We use the method of Worked Exercise B41.

$$(a) \ (1 \ 8 \ 3)(2 \ 6 \ 5 \ 7) \\ = (1 \ 8 \ 3) \circ (2 \ 6 \ 5 \ 7) \\ = (1 \ 3) \circ (1 \ 8) \circ (2 \ 7) \circ (2 \ 5) \circ (2 \ 6).$$

$$(b) \ (1 \ 7)(2 \ 6 \ 8)(3 \ 4 \ 5) \\ = (1 \ 7) \circ (2 \ 6 \ 8) \circ (3 \ 4 \ 5) \\ = (1 \ 7) \circ (2 \ 8) \circ (2 \ 6) \circ (3 \ 5) \circ (3 \ 4).$$

Solution to Exercise B109

(a) We apply Theorem B59.

The permutation $(1 \ 2 \ 5 \ 3)$ is a 4-cycle and so is odd.

The permutation $(1 \ 6 \ 2 \ 5 \ 4)$ is a 5-cycle and so is even.

(b) The solution to Exercise B108 shows that the permutation $(1 \ 8 \ 3)(2 \ 6 \ 5 \ 7)$ can be expressed as a composite of five transpositions and so is an odd permutation.

It also shows that the permutation $(1 \ 7)(2 \ 6 \ 8)(3 \ 4 \ 5)$ can be expressed as a composite of five transpositions and so is an odd permutation.

(c) We use Strategy B10 to express the two cycles as composites of transpositions. This gives

$$(1 \ 8 \ 2 \ 7 \ 6)(3 \ 5 \ 9 \ 4) \\ = (1 \ 8 \ 2 \ 7 \ 6) \circ (3 \ 5 \ 9 \ 4) \\ = (1 \ 6) \circ (1 \ 7) \circ (1 \ 2) \circ (1 \ 8) \circ (3 \ 4) \circ (3 \ 9) \circ (3 \ 5).$$

So $(1 \ 8 \ 2 \ 7 \ 6)(3 \ 5 \ 9 \ 4)$ can be expressed as a composite of seven transpositions and so is an odd permutation.

Solution to Exercise B110

(a) Here

$$(1 \ 2 \ 4)(3 \ 5) \circ (1 \ 5 \ 2) = (1 \ 2 \ 4) \circ (3 \ 5) \circ (1 \ 5 \ 2).$$

The cycles of the expression on the right-hand side of this equation are respectively even, odd and even. Combining parities we obtain

$$\text{even} + \text{odd} + \text{even} = \text{odd}.$$

Thus $(1 \ 2 \ 4)(3 \ 5) \circ (1 \ 5 \ 2)$ is an odd permutation.

(b) Here

$$(1 \ 2 \ 4) \circ (1 \ 3)(2 \ 5 \ 4) \circ (1 \ 2 \ 3 \ 4) \\ = (1 \ 2 \ 4) \circ (1 \ 3) \circ (2 \ 5 \ 4) \circ (1 \ 2 \ 3 \ 4).$$

The cycles of the expression on the right-hand side of this equation are respectively even, odd, even and odd, so we obtain

$$\text{even} + \text{odd} + \text{even} + \text{odd} = \text{even}.$$

Thus $(1 \ 2 \ 4) \circ (1 \ 3)(2 \ 5 \ 4) \circ (1 \ 2 \ 3 \ 4)$ is an even permutation.

Solution to Exercise B111

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}.$$

(The other three elements of S_3 are the transpositions, which are odd permutations.)

Thus A_3 has order 3.

Solution to Exercise B112

(a) The cycle number of f is 1.

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 4\ 5\ 2\ 3\ 6\ 7) \\ &= (1\ 4\ 5)(2\ 3\ 6\ 7) \end{aligned}$$

So the cycle number of $t \circ f$ is 2.

(b) The cycle number of f is 2.

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 4\ 3)(2\ 6\ 5\ 7) \\ &= (1\ 4\ 3\ 2\ 6\ 5\ 7) \end{aligned}$$

So the cycle number of $t \circ f$ is 1.

(c) The cycle number of f is 3. (Since f is $(1\ 2\ 7\ 3)(4\ 6)(5)$ with 1-cycles included.)

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 2\ 7\ 3)(4\ 6) \\ &= (1)(2\ 7\ 3)(4\ 6) \\ &= (2\ 7\ 3)(4\ 6) \end{aligned}$$

So the cycle number of $t \circ f$ is 4. (It has a 3-cycle, a 2-cycle and two 1-cycles.)

(d) The cycle number of f is 3.

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 5\ 3)(2\ 4)(6\ 7) \\ &= (1\ 5\ 3\ 2\ 4)(6\ 7) \end{aligned}$$

So the cycle number of $t \circ f$ is 2.

Solution to Exercise B113

The original permutations are as follows.

Rotations	Reflections
e	$(1\ 4)(2\ 3)$
$(1\ 2\ 3\ 4)$	$(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$
$(1\ 4\ 3\ 2)$	$(1\ 3)$

(a) The permutations obtained by relabelling the vertex locations using the transposition $(3\ 4)$, that is, by interchanging 3 and 4, are as follows.

Rotations	Reflections
e	$(1\ 3)(2\ 4)$
$(1\ 2\ 4\ 3)$	$(2\ 3)$
$(1\ 4)(2\ 3)$	$(1\ 2)(4\ 3)$
$(1\ 3\ 4\ 2)$	$(1\ 4)$

(b) The permutations obtained by relabelling the vertex locations using the permutation $(2\ 3\ 4)$, that is, by keeping 1 fixed and replacing 2 by 3, 3 by 4 and 4 by 2, are as follows.

Rotations	Reflections
e	$(1\ 2)(3\ 4)$
$(1\ 3\ 4\ 2)$	$(3\ 2)$
$(1\ 4)(3\ 2)$	$(1\ 3)(4\ 2)$
$(1\ 2\ 4\ 3)$	$(1\ 4)$

Here one of the reflections, $(3\ 2)$, is not written in the usual way. If we write it in the usual way, then we obtain the following list of permutations.

Rotations	Reflections
e	$(1\ 2)(3\ 4)$
$(1\ 3\ 4\ 2)$	$(2\ 3)$
$(1\ 4)(3\ 2)$	$(1\ 3)(4\ 2)$
$(1\ 2\ 4\ 3)$	$(1\ 4)$

(Notice that the list of permutations found in part (b) is in fact exactly the same as the list found in part (a).)

Solution to Exercise B114

(a) Here $g = (1\ 4)(2\ 5\ 3)$, so $g^{-1} = (4\ 1)(3\ 5\ 2)$ which, when rewritten in the usual way, is $(1\ 4)(2\ 3\ 5)$. Thus

$$\begin{aligned} g \circ x \circ g^{-1} &= (1\ 4)(2\ 5\ 3) \circ (1\ 2\ 3\ 5) \circ (1\ 4)(2\ 3\ 5) \\ &= (1)(2\ 3\ 4\ 5) \\ &= (2\ 3\ 4\ 5). \end{aligned}$$

Using $g = (1\ 4)(2\ 5\ 3)$ to rename $x = (1\ 2\ 3\ 5)$, we obtain $(4\ 5\ 2\ 3)$, which is the same 4-cycle as above.

(b) Here $g = (1\ 3\ 4\ 2\ 5)$, so $g^{-1} = (5\ 2\ 4\ 3\ 1)$ which, when rewritten in the usual way, is $(1\ 5\ 2\ 4\ 3)$. Thus

$$\begin{aligned} g \circ x \circ g^{-1} &= (1\ 3\ 4\ 2\ 5) \circ (1\ 2\ 3\ 5) \circ (1\ 5\ 2\ 4\ 3) \\ &= (1\ 3\ 5\ 4)(2) \\ &= (1\ 3\ 5\ 4). \end{aligned}$$

Using $g = (1\ 3\ 4\ 2\ 5)$ to rename $x = (1\ 2\ 3\ 5)$, we obtain $(3\ 5\ 4\ 1)$, which is the same 4-cycle as above.

Solution to Exercise B115

We obtain three more answers by writing y in the following three ways:

$$(2\ 5\ 3)(4\ 1), \quad (3\ 2\ 5)(4\ 1), \quad (5\ 3\ 2)(1\ 4).$$

With the first way above we obtain

$$\begin{aligned} x &= (1\ 2\ 4)(3\ 5) \\ g \downarrow \quad \downarrow \downarrow \downarrow \downarrow \downarrow, \\ y &= (2\ 5\ 3)(4\ 1) \end{aligned}$$

which gives $g = (1\ 2\ 5)(3\ 4)$.

With the second way we obtain

$$\begin{aligned} x &= (1\ 2\ 4)(3\ 5) \\ g \downarrow \quad \downarrow \downarrow \downarrow \downarrow \downarrow, \\ y &= (3\ 2\ 5)(4\ 1) \end{aligned}$$

which gives $g = (1\ 3\ 4\ 5)$.

Finally, with the third way we obtain

$$\begin{aligned} x &= (1\ 2\ 4)(3\ 5) \\ g \downarrow \quad \downarrow \downarrow \downarrow \downarrow \downarrow, \\ y &= (5\ 3\ 2)(1\ 4) \end{aligned}$$

which gives $g = (1\ 5\ 4\ 2\ 3)$.

Solution to Exercise B116

(a) Here $x = (1\ 2\ 3\ 4)(5)$ and $y = (1\ 5\ 2\ 3)(4)$. We can write the cycle in $(1\ 5\ 2\ 3)$ in y in four ways:

$$(1\ 5\ 2\ 3), \quad (5\ 2\ 3\ 1), \quad (2\ 3\ 1\ 5), \quad (3\ 1\ 5\ 2).$$

Writing y as $(1\ 5\ 2\ 3)(4)$ and matching up the cycles we obtain

$$\begin{aligned} x &= (1\ 2\ 3\ 4)(5) \\ g \downarrow \quad \downarrow \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (2\ 5\ 4\ 3). \\ y &= (1\ 5\ 2\ 3)(4) \end{aligned}$$

Similarly, for the other three ways of writing y we obtain

$$\begin{aligned} x &= (1\ 2\ 3\ 4)(5) \\ g \downarrow \quad \downarrow \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 5\ 4); \\ y &= (5\ 2\ 3\ 1)(4) \\ x &= (1\ 2\ 3\ 4)(5) \\ g \downarrow \quad \downarrow \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 2\ 3)(4\ 5); \\ y &= (2\ 3\ 1\ 5)(4) \\ x &= (1\ 2\ 3\ 4)(5) \\ g \downarrow \quad \downarrow \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 3\ 5\ 4\ 2). \\ y &= (3\ 1\ 5\ 2)(4) \end{aligned}$$

(b) There are eight different ways of writing the permutation $(1\ 2)(3\ 4)$ underneath itself with the cycles matched up. (There are 2 ways to write each of the two cycles, and 2 ways to order the two cycles, so the number of suitable ways to write the permutation is $2 \times 2 \times 2 = 8$.)

Writing it in these eight possible ways we obtain

$$\begin{aligned} (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= e; \\ (1\ 2)(3\ 4) \\ (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 2); \\ (2\ 1)(3\ 4) \\ (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (3\ 4); \\ (1\ 2)(4\ 3) \\ (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 2)(3\ 4); \\ (2\ 1)(4\ 3) \\ (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 3)(2\ 4); \\ (3\ 4)(1\ 2) \\ (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 4\ 2\ 3); \\ (4\ 3)(1\ 2) \\ (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 3\ 2\ 4); \\ (3\ 4)(2\ 1) \\ (1\ 2)(3\ 4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g &= (1\ 4)(2\ 3). \\ (4\ 3)(2\ 1) \end{aligned}$$

Solution to Exercise B117

(a) Renaming the symbols in each permutation in H using the permutation $g = (1\ 4)(2\ 5)$ gives

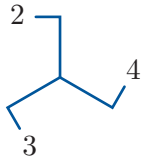
$$\begin{aligned} g \circ H \circ g^{-1} &= \{e, (4\ 3\ 2), (4\ 2\ 3)\} \\ &= \{e, (2\ 4\ 3), (2\ 3\ 4)\}. \end{aligned}$$

(b) The set $g \circ H \circ g^{-1}$ is a subgroup of S_5 because it is the cyclic subgroup of S_5 generated by the 3-cycle $(2\ 4\ 3)$:

$$\begin{aligned} \langle (2\ 4\ 3) \rangle &= \{e, (2\ 4\ 3), (2\ 4\ 3)^2\} \\ &= \{e, (2\ 4\ 3), (2\ 3\ 4)\} \\ &= g \circ H \circ g^{-1}. \end{aligned}$$

(There are other ways to show that $g \circ H \circ g^{-1}$ is a subgroup of S_5 . For example, you could construct a Cayley table for this set and use the usual subgroup test (Theorem B24 in Unit B2).

Alternatively, you could argue that the elements of the set $g \circ H \circ g^{-1}$ represent the symmetries of the labelled figure below, with the symbols 1 and 5 being fixed.)



Solution to Exercise B118

Here $H = \{e, (1\ 2\ 5\ 3), (1\ 5)(2\ 3), (1\ 3\ 5\ 2)\}$.

(a) To find $(1\ 3) \circ H \circ (1\ 3)^{-1}$ we interchange the symbols 1 and 3 in the elements of H , which gives

$$\begin{aligned} (1\ 3) \circ H \circ (1\ 3)^{-1} &= \{e, (3\ 2\ 5\ 1), (3\ 5)(2\ 1), (3\ 1\ 5\ 2)\} \\ &= \{e, (1\ 3\ 2\ 5), (1\ 2)(3\ 5), (1\ 5\ 2\ 3)\}. \end{aligned}$$

(b) To find $(1\ 3)(2\ 4) \circ H \circ ((1\ 3)(2\ 4))^{-1}$ we replace 1 by 3, 3 by 1, 2 by 4 and 4 by 2 in the elements of H , which gives

$$\begin{aligned} (1\ 3)(2\ 4) \circ H \circ ((1\ 3)(2\ 4))^{-1} &= \{e, (3\ 4\ 5\ 1), (3\ 5)(4\ 1), (3\ 1\ 5\ 4)\} \\ &= \{e, (1\ 3\ 4\ 5), (1\ 4)(3\ 5), (1\ 5\ 4\ 3)\}. \end{aligned}$$

Solution to Exercise B119

(a) There are three permutations g that conjugate $(1\ 2\ 3)$ to itself, corresponding to the three ways of writing $(1\ 2\ 3)$, as shown in the following table.

Form of $(1\ 2\ 3)$	Conjugating permutation
$(1\ 2\ 3)$	e
$(2\ 3\ 1)$	$(1\ 2\ 3)$
$(3\ 1\ 2)$	$(1\ 3\ 2)$

These three conjugating permutations are the elements of the subgroup A_3 of S_3 .

(An alternative way to show that the three conjugating permutations above form a subgroup of S_3 is to show that they are the elements of the cyclic subgroup of S_3 generated by the permutation $(1\ 2\ 3)$.)

(b) There are four permutations g that conjugate $(1\ 2\ 3\ 4)$ to itself, corresponding to the four ways of writing $(1\ 2\ 3\ 4)$, as shown in the following table.

Form of $(1\ 2\ 3\ 4)$	Conjugating permutation
$(1\ 2\ 3\ 4)$	e
$(2\ 3\ 4\ 1)$	$(1\ 2\ 3\ 4)$
$(3\ 4\ 1\ 2)$	$(1\ 3)(2\ 4)$
$(4\ 1\ 2\ 3)$	$(1\ 4\ 3\ 2)$

Now $(1\ 2\ 3\ 4)$ has order 4 and

$$\begin{aligned} (1\ 2\ 3\ 4)^2 &= (1\ 2\ 3\ 4) \circ (1\ 2\ 3\ 4), \\ &= (1\ 3)(2\ 4), \end{aligned}$$

$$\begin{aligned} (1\ 2\ 3\ 4)^3 &= (1\ 2\ 3\ 4) \circ (1\ 2\ 3\ 4)^2 \\ &= (1\ 2\ 3\ 4) \circ (1\ 3)(2\ 4) \\ &= (1\ 4\ 3\ 2). \end{aligned}$$

So the four conjugating permutations form the cyclic subgroup of S_4 generated by $(1\ 2\ 3\ 4)$:

$$\begin{aligned} &\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\} \\ &= \langle (1\ 2\ 3\ 4) \rangle. \end{aligned}$$

Solution to Exercise B120

We show that C satisfies the three subgroup properties SG1, SG2 and SG3.

SG1 Let g_1 and g_2 be any two elements of C ; then

$$g_1 \circ f \circ g_1^{-1} = f$$

and

$$g_2 \circ f \circ g_2^{-1} = f.$$

Substituting the second of these equations into the first gives

$$g_1 \circ g_2 \circ f \circ g_2^{-1} \circ g_1^{-1} = f;$$

that is (by Proposition B14 in Unit B1),

$$(g_1 \circ g_2) \circ f \circ (g_1 \circ g_2)^{-1} = f.$$

This shows that $g_1 \circ g_2$ is in C , so C is closed under \circ .

SG2 We have $e \circ f \circ e^{-1} = f$, so $e \in C$.

SG3 Let g be any element of C ; then

$$g \circ f \circ g^{-1} = f.$$

Composing both sides of this equation on the left by g^{-1} and on the right by g gives

$$g^{-1} \circ g \circ f \circ g^{-1} \circ g = g^{-1} \circ f \circ g.$$

This equation simplifies to give

$$f = g^{-1} \circ f \circ g,$$

which can be written as

$$g^{-1} \circ f \circ (g^{-1})^{-1} = f.$$

This shows that g^{-1} is in C , so C contains the inverse of each of its elements.

Hence C satisfies the three subgroup properties and so is a subgroup of G .

(The condition $g \circ f \circ g^{-1} = f$ is equivalent to the condition $g \circ f = f \circ g$, so C is the set of all elements of G that *commute* with the fixed element f . If x and y are elements of a group (G, \circ) , then we say that x *commutes* with y if $x \circ y = y \circ x$.)

Solution to Exercise B121

Here

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Let $g \in S_4$. Then

$$\begin{aligned} g \circ H \circ g^{-1} \\ = \{g \circ e \circ g^{-1}, g \circ (1\ 2)(3\ 4) \circ g^{-1}, \\ g \circ (1\ 3)(2\ 4) \circ g^{-1}, g \circ (1\ 4)(2\ 3) \circ g^{-1}\}. \end{aligned}$$

Now $g \circ e \circ g^{-1} = e$.

Also, we know that

$$g \circ (1\ 2)(3\ 4) \circ g^{-1}$$

is a permutation in S_4 with the same cycle structure as $(1\ 2)(3\ 4)$, so it must be one of the permutations $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$; that is, it must be one of the three non-identity permutations in H . The same argument holds for each of the remaining two conjugates in $g \circ H \circ g^{-1}$.

To complete the proof we have to show that no two of the three permutations

$$\begin{aligned} g \circ (1\ 2)(3\ 4) \circ g^{-1}, \\ g \circ (1\ 3)(2\ 4) \circ g^{-1}, \\ g \circ (1\ 4)(2\ 3) \circ g^{-1} \end{aligned}$$

are equal to the *same* non-identity permutation in H .

This is the case because, by the Cancellation Laws, if x and y are any two elements of S_n , then

$$g \circ x \circ g^{-1} = g \circ y \circ g^{-1}$$

gives $x = y$.

So the four elements of $g \circ H \circ g^{-1}$ are precisely the four elements of H . That is,

$$g \circ H \circ g^{-1} = H.$$

Solution to Exercise B122

(a) The only cyclic subgroup of order 1 is $\{e\}$. Each cyclic subgroup of order 2 consists of the identity permutation together with one permutation of order 2. Thus the cyclic subgroups of S_4 of order 2 are:

$\{e, (1\ 2)\}, \{e, (1\ 3)\}, \{e, (1\ 4)\},$
 $\{e, (2\ 3)\}, \{e, (2\ 4)\}, \{e, (3\ 4)\},$
 $\{e, (1\ 2)(3\ 4)\}, \{e, (1\ 3)(2\ 4)\}, \{e, (1\ 4)(2\ 3)\}.$

We now find the cyclic subgroups of S_4 of order 4. The cyclic subgroup generated by the permutation $(1\ 2\ 3\ 4)$ is

$\langle (1\ 2\ 3\ 4) \rangle = \{e, (1\ 2\ 3\ 4), (1\ 2\ 3\ 4) \circ (1\ 2\ 3\ 4),$
 $(1\ 2\ 3\ 4) \circ (1\ 2\ 3\ 4) \circ (1\ 2\ 3\ 4)\}$
 $= \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}.$

This subgroup contains two permutations of order 4.

We now choose a permutation of order 4 that is not one of these two and find, in the same way as above, the cyclic subgroup that it generates:

$\langle (1\ 2\ 4\ 3) \rangle = \{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}.$

Next we choose a permutation of order 4 that is not one of the four such permutations appearing in the two subgroups of order 4 found already and find the cyclic subgroup that it generates:

$\langle (1\ 3\ 2\ 4) \rangle = \{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}.$

We have now dealt with all six permutations of order 4 in S_4 , so we have found all the cyclic subgroups of S_4 of order 4.

(b) The numbers of cyclic subgroups of S_4 of each order can be summarised as follows.

Order	Number of cyclic subgroups
1	1
2	9
3	4
4	3

Solution to Exercise B123

(a) Using the labelling on the figures in the usual way, we obtain the following symmetry groups.

- (i) $\{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$
- (ii) $\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$
- (iii) $\{e, (1\ 2)\}$
- (iv) $\{e, (1\ 3), (1\ 4), (3\ 4), (1\ 3\ 4), (1\ 4\ 3)\}$
- (b) The subgroups in parts (a)(ii) and (iii) are cyclic, because they are generated by the permutations $(1\ 2\ 3\ 4)$ and $(1\ 2)$, respectively. The other two subgroups are non-cyclic. The subgroup in part (a)(i) has order 4, but contains no element of order 4. The subgroup in part (a)(iv) has order 6, but contains no element of order 6.

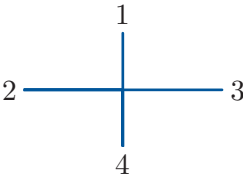
Solution to Exercise B124

(a) We obtain the following subgroup of S_4 :

$\{e, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}.$

(You can find the elements of this subgroup either directly from the figure or by renaming the symbols in the permutations in the subgroup found in Exercise B123(a)(i) using the transposition $(2\ 3)$.)

(b) We can relabel the figure as follows.

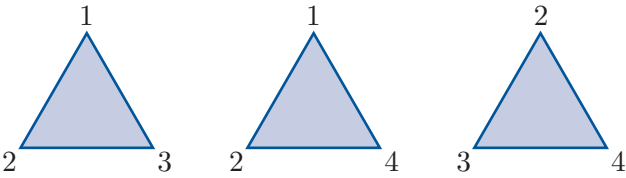


We obtain the following subgroup of S_4 :

$\{e, (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}.$

Solution to Exercise B125

We can relabel the triangle in the following three ways.

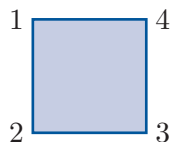


We obtain the following three subgroups of S_4 :

$\{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\},$
 $\{e, (1\ 2), (1\ 4), (2\ 4), (1\ 2\ 4), (1\ 4\ 2)\},$
 $\{e, (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}.$

Solution to Exercise B126

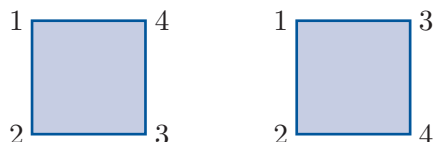
(a) We can use the symmetry group of the square. One way to label the square is as follows.



This gives the following subgroup of S_4 :

$$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 4)(2\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 3)\}.$$

(b) We can relabel the square in the two other ways shown below. In the first we interchange the symbols 2 and 3; in the second we interchange 3 and 4.



We obtain the following two subgroups of S_4 :

$$\begin{aligned} &\{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3), \\ &\quad (1\ 4)(2\ 3), (3\ 4), (1\ 3)(2\ 4), (1\ 2)\}, \\ &\{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2), \\ &\quad (1\ 3)(2\ 4), (2\ 3), (1\ 2)(3\ 4), (1\ 4)\}. \end{aligned}$$

(Notice that although there are other ways of relabelling the vertices of the square, these do not give any more subgroups. For example, interchanging the symbols 1 and 4 leads to the same subgroup as interchanging 2 and 3. In fact we have already found the three subgroups above, at the start of Subsection 4.1.)

Solution to Exercise B127

(a) Not all subgroups of S_4 of order 2 are conjugate to each other.

For example, the subgroups $\{e, (1\ 2)\}$ and $\{e, (1\ 2)(3\ 4)\}$ are not conjugate because the cycle structures of their elements do not match.

(b) All subgroups of S_4 of order 3 are conjugate to each other.

We have seen that the subgroups of S_4 of order 3 are

$$\begin{aligned} &\{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\ &\{e, (1\ 2\ 4), (1\ 4\ 2)\}, \\ &\{e, (1\ 3\ 4), (1\ 4\ 3)\}, \\ &\{e, (2\ 3\ 4), (2\ 4\ 3)\}. \end{aligned}$$

The first of these subgroups is conjugated to the other three by, for example, the permutations $(3\ 4)$, $(2\ 4)$ and $(1\ 4)$, respectively. (There are other conjugating permutations, of course.)

Solution to Exercise B128

(a) The subgroup $\{e, (1\ 3\ 4), (1\ 4\ 3)\}$ is the group of direct symmetries of the tetrahedron that fix the vertex at location 2; that is, the group of rotations about an axis passing through the vertex at location 2 and the middle of the opposite face.

(b) The subgroup $\{e, (3\ 4)\}$ is the subgroup generated by the reflection of the tetrahedron in the plane through the edge joining the vertices at locations 1 and 2 and the midpoint of the edge joining the vertices at locations 3 and 4.

(c) The subgroup

$$\{e, (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}$$

is the group of all symmetries of the tetrahedron fixing the vertex at location 1; that is, the group of symmetries of the equilateral triangle with vertices at locations 2, 3 and 4.

(d) The subgroup $\{e, (1\ 2)(3\ 4)\}$ is the subgroup generated by the rotation through π about the line that passes through the midpoint of the edge joining the vertices at locations 1 and 2 and the midpoint of the edge joining the vertices at locations 3 and 4.

Solution to Exercise B129

Using the method of Worked Exercise B47 we obtain the following permutations.

\circ	e	a	b	c	p	q	r	s	
e	e	a	b	c	p	q	r	s	$\longrightarrow i$ (identity)
a	a	e	c	b	q	p	s	r	$\longrightarrow (e\ a)(b\ c)(p\ q)(r\ s)$
b	b	c	a	e	r	s	q	p	$\longrightarrow (e\ b\ a\ c)(p\ r\ q\ s)$
c	c	b	e	a	s	r	p	q	$\longrightarrow (e\ c\ a\ b)(p\ s\ q\ r)$
p	p	q	s	r	a	e	b	c	$\longrightarrow (e\ p\ a\ q)(b\ s\ c\ r)$
q	q	p	r	s	e	a	c	b	$\longrightarrow (e\ q\ a\ p)(b\ r\ c\ s)$
r	r	s	p	q	c	b	a	e	$\longrightarrow (e\ r\ a\ s)(b\ p\ c\ q)$
s	s	r	q	p	b	c	e	a	$\longrightarrow (e\ s\ a\ r)(b\ q\ c\ p)$

Hence a permutation group isomorphic to the given group is

$$\{i, (e\ a)(b\ c)(p\ q)(r\ s), (e\ b\ a\ c)(p\ r\ q\ s), \\ (e\ c\ a\ b)(p\ s\ q\ r), (e\ p\ a\ q)(b\ s\ c\ r), \\ (e\ q\ a\ p)(b\ r\ c\ s), (e\ r\ a\ s)(b\ p\ c\ q), \\ (e\ s\ a\ r)(b\ q\ c\ p)\},$$

where i is the identity permutation.

Solution to Exercise B130

We have $U_8 = \{1, 3, 5, 7\}$.

We construct the group table for (U_8, \times_8) , then from each row we determine, in cycle form, the corresponding permutation of the column headings.

\times_8	1	3	5	7	
1	1	3	5	7	$\longrightarrow (1)(3)(5)(7) = e$
3	3	1	7	5	$\longrightarrow (1\ 3)(5\ 7)$
5	5	7	1	3	$\longrightarrow (1\ 5)(3\ 7)$
7	7	5	3	1	$\longrightarrow (1\ 7)(3\ 5)$

Hence a permutation group isomorphic to the group (U_8, \times_8) is

$$\{e, (1\ 3)(5\ 7), (1\ 5)(3\ 7), (1\ 7)(3\ 5)\}.$$

(The group table for (U_8, \times_8) above shows that (U_8, \times_8) has four elements all of which are self-inverse, and hence is isomorphic to the Klein four-group V . So in fact any permutation group isomorphic to V will do as the solution to this exercise, such as the symmetry group of the rectangle when the symmetries are represented as permutations.)

Unit B4

Lagrange's Theorem and small groups

Introduction

This unit rounds off this book with three separate topics.

In Section 1 you will meet *Lagrange’s Theorem*, a powerful result that relates the orders of the subgroups of a group to the order of the group. You will see some simple but important corollaries of this result.

In Section 2 you will see how we can use Lagrange’s Theorem, its corollaries and some other results proved earlier in this book to determine all the possible structures – that is, all the isomorphism classes – for groups of orders 1 to 7. The isomorphism classes for groups of order 8 are also described, without proof.

Section 3 is a little different from the rest of this book. It does not cover any significant new group theory, but instead gives you a chance, within the topic of group theory, to improve your skills in understanding theorems and proofs, and in producing your own proofs. These are skills that are extremely important in pure mathematics and will be needed in the rest of the module, particularly in Book E *Group theory 2* and in the analysis books (Books D and F). You will practise these skills by revisiting some of the results in group theory you have already met, and proving a few more.

1 Lagrange’s Theorem

In this section you will meet one of the most important results in group theory – Lagrange’s Theorem.

1.1 Orders of subgroups of a group

In Unit B2 *Subgroups and isomorphisms* we found various subgroups of the group $S(\square)$, whose non-identity elements are shown in Figure 1. In fact, we found all the subgroups of $S(\square)$, though we are not in a position to prove this at the moment. They are listed in Table 1. Remember that the **order** of a group or subgroup is the number of elements that it contains.

Table 1 The subgroups of the symmetry group $S(\square)$

Order	Number of subgroups	Subgroups
1	1	$\{e\}$
2	5	$\{e, b\}, \{e, r\}, \{e, s\}, \{e, t\}, \{e, u\}$
4	3	$\{e, a, b, c\}, \{e, b, r, t\}, \{e, b, s, u\}$
8	1	$S(\square)$

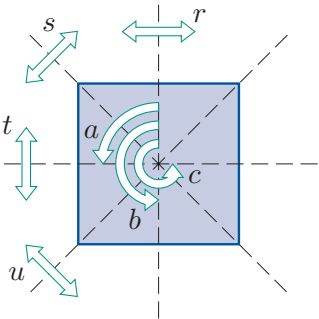


Figure 1 $S(\square)$

The subgroups in Table 1 are $S(\square)$ itself, all its cyclic subgroups, and two non-cyclic subgroups of order 4 that we found by modifying the square (see Subsection 1.3 of Unit B2). Notice that each of the subgroups of $S(\square)$ has an order that divides 8, the order of $S(\square)$. (An integer a is said to **divide** an integer b if a is a factor of b .) We did not find any subgroups of $S(\square)$ of orders 3, 5, 6 or 7.

Also, in Section 5 of Unit B3 *Permutations* we found all the subgroups of the symmetric group S_4 . Our findings are summarised in Table 2, which is repeated from Unit B3.

Table 2 The subgroups of the symmetric group S_4

Order	Number of subgroups	Description
1	1	$\{e\}$
2	9	all cyclic
3	4	all cyclic
4	7	3 cyclic; 4 Klein
6	4	all isomorphic to $S(\triangle)$
8	3	all isomorphic to $S(\square)$
12	1	A_4
24	1	S_4

You can see from Table 2 that each subgroup of S_4 has an order that divides 24, the order of S_4 .

So, for both $S(\square)$ and S_4 , the order of each subgroup divides the order of the group. Lagrange's Theorem states that this is true for finite groups in general.

Theorem B68 Lagrange's Theorem

Let G be a finite group and let H be any subgroup of G . Then the order of H divides the order of G .

For example, if G is a group of order 12, then any subgroup of G has order 1, 2, 3, 4, 6 or 12. These numbers are the positive factors, also called the positive **divisors**, of 12. This group G cannot have a subgroup of order 5, 7, 8, 9, 10 or 11.

Exercise B131

Let G be a group of order n and let H be a subgroup of G . List all the possible orders of H in each of the following cases.

(a) $n = 20$ (b) $n = 25$ (c) $n = 29$

Notice that the group in the statement of Lagrange's Theorem above is referred to simply as G , without mention of its binary operation, rather than as (G, \circ) . It is often convenient to use this more concise notation in theorems or discussions about abstract groups, and we will do so throughout this section. This is part of a commonly used convention for notation for abstract groups that is explained more fully in the next section. (By an *abstract* group we mean one that is not a specific, concrete group such as $S(\square)$ or S_4 .)

A proof of Lagrange's Theorem follows shortly. It proves the theorem by showing that if G is any finite group and H is any subgroup of G , then it is always possible to arrange the elements of G in the form of a rectangular array with the elements of H as the first row, as illustrated in Figure 2. The order of G is then the number of elements in the array, which is equal to the number of rows of the array times the number of columns of the array. Since the number of columns of the array is the order of H , it follows immediately that the order of H divides the order of G .

The proof describes a method for arranging the elements of the group G in such an array. It is helpful for you to see the method in action before you read the proof, so here is how it is carried out for the group $S(\square)$ and its 2-element subgroup $H = \langle r \rangle = \{e, r\}$. We start by writing the elements of H as the first row of the array, as follows.

$$e \quad r$$

Then we take any element of $S(\square)$ that does not appear in this row: we can choose a , for example. We compose each of the elements of H on the left with this new element to form the composite elements $a \circ e = a$ and $a \circ r = s$ (see Table 3), and write these composites below the elements of H to form a second row of the array, as follows.

$$\begin{array}{cc} e & r \\ a & s \end{array}$$

Next we take any element of $S(\square)$ that is not already in the array: we can choose b , for example. Again we compose each of the elements of H on the left with this new element to form the composite elements $b \circ e = b$ and $b \circ r = t$, and write down these composites to form a third row of the array, as follows.

$$\begin{array}{cc} e & r \\ a & s \\ b & t \end{array}$$

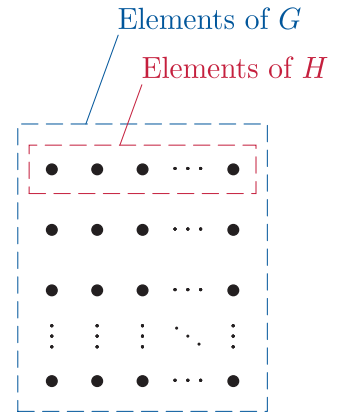


Figure 2 An arrangement of the elements of a group G with a subgroup H as the first row

Table 3 $S(\square)$

\circ	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

We continue in this way until every element of $S(\square)$ appears in the array. So next we take any element of $S(\square)$ that is not already in the array: we can choose c , for example. We compose each of the elements of H on the left with this new element to form the composite elements $c \circ e = c$ and $c \circ r = u$, and write down these composites to form a fourth row of the array, as follows.

e	r
a	s
b	t
c	u

Now every element of $S(\square)$ appears in the array, so the array is complete. It has the properties that we wanted: it is an arrangement of the elements of $S(\square)$, and it has the subgroup H as its first row.

The method that we used above must certainly produce a rectangular array of elements of $S(\square)$ with the elements of the subgroup H as the first row. However, it was not clear from the start that the array would definitely turn out to be an *arrangement of the elements of $S(\square)$* – perhaps it was just luck that no elements of $S(\square)$ appear more than once in the array? In the proof of Lagrange’s Theorem you will see that it was not just luck: the method never gives repeated elements.

You can try the method for yourself in the next exercise.

Exercise B132

Table 4 $S(\square)$

\circ	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

For each of the following subgroups of $S(\square)$, use the method demonstrated above to arrange the elements of $S(\square)$ in the form of a rectangular array whose first row consists of the elements of the subgroup. To find the necessary composites of elements of $S(\square)$, use the Cayley table of $S(\square)$, given as Table 4.

- (a) $\{e, b\}$
- (b) $\{e, a, b, c\}$

As mentioned earlier, it is not immediately obvious that the method demonstrated above always produces an array in which the elements are all *distinct* – and we certainly need them to be distinct so that the number of elements in the array is the order of the group that we started with. How do we know that the elements in each row will always turn out to be all different from each other, for example? And how do we know that an element obtained in one row is never repeated in another row?

The proof of Lagrange’s Theorem given below describes the method demonstrated above for arranging the elements of a group G given a subgroup H , and shows that the elements of G in the resulting array are indeed always distinct. You may think the proof looks rather long, but this should not deter you from reading it: the first half of it is just the description of the method demonstrated above.

Proof of Lagrange's Theorem Let G be a finite group with binary operation \circ , and let H be any subgroup of G .

Let the order of H be r , and let $H = \{h_1, h_2, \dots, h_r\}$. We form an array of elements of G by using the following procedure.

We start by writing the elements of H as the first row of the array:

$$h_1 \quad h_2 \quad \dots \quad h_r.$$

If there are no elements of G not yet placed in the array (that is, if $H = G$), then the array is complete. Otherwise, we choose any element of G that is not yet in the array, say g_2 (the subscript 2 has been chosen for convenience, to correspond to row 2), compose each of the elements of H on the left with this new element, and write down the resulting r composites to form the second row of the array:

$$\begin{array}{cccc} h_1 & h_2 & \dots & h_r \\ g_2 \circ h_1 & g_2 \circ h_2 & \dots & g_2 \circ h_r. \end{array}$$

If there are no elements of G not yet placed in the array, then the array is complete. Otherwise, we choose any element of G that is not yet in the array, say g_3 , compose each of the elements of H on the left with this new element, and write down the resulting r composites to form the third row of the array:

$$\begin{array}{cccc} h_1 & h_2 & \dots & h_r \\ g_2 \circ h_1 & g_2 \circ h_2 & \dots & g_2 \circ h_r \\ g_3 \circ h_1 & g_3 \circ h_2 & \dots & g_3 \circ h_r. \end{array}$$

We continue appending new rows in this way until all the elements of G appear in the array. This must happen, because each new row

$$g_k \circ h_1 \quad g_k \circ h_2 \quad \dots \quad g_k \circ h_r$$

contains the element g_k (because one of h_1, h_2, \dots, h_r is the identity element), and g_k does not appear in any previous row. So each new row includes at least one element that does not appear in any previous row.

We now show that the elements of G in the array are all distinct.

First we show that in each row of the array the r elements are all distinct. Certainly the r elements in the first row are all distinct, because they are the r elements of H . Also, the r elements in each subsequent row are all distinct, because if

$$g_k \circ h_i = g_k \circ h_j$$

for some $g_k \in G$ and $h_i, h_j \in H$, then, by the Left Cancellation Law,

$$h_i = h_j,$$

that is, h_i and h_j are the same element of H .

Next we show that none of the elements in each new row of the array is a repeat of an element that appeared in a previous row. We use a contradiction argument. Suppose that in some row, say row l , there is an element $g_l \circ h_i$ that is a repeat of an element $g_k \circ h_j$ that appeared in row k , a previous row. Then

$$g_l \circ h_i = g_k \circ h_j.$$

Composing each side of this equation on the right by h_i^{-1} gives

$$g_l = g_k \circ h_j \circ h_i^{-1}.$$

Now $h_j \circ h_i^{-1} \in H$, since H is a subgroup, so the equation above implies that the element g_l appears in row k of the array. This is a contradiction, because we chose g_l to be an element that does not appear in a previous row. Thus none of the elements in each new row of the array is a repeat of an element that appeared in a previous row. The argument here applies even if row k is the first row, since we can write the first row as

$$g_1 \circ h_1 \quad g_1 \circ h_2 \quad \dots \quad g_1 \circ h_r,$$

where $g_1 = e$.

Thus all the elements of G in the array are distinct, and hence the order of G is equal to the number of elements in the array, which is equal to the number of rows of the array times the number of columns of the array. But the number of columns of the array is r , the order of H , so the order of H divides the order of G . ■

In Book E you will see that the elements in each row of the array described in the proof above form a set known as a *left coset* of the subgroup H in the group G . Left cosets, and also right cosets, which are obtained in exactly the same way but by composing with the new elements on the right instead of the left, are hugely important in group theory, and you will learn about them, and many of their properties and uses, in Book E.

Lagrange's Theorem allows us to write down all the *possible* orders for subgroups of a finite group G – these are all the positive divisors of the order of G . Thus, if the natural number m does *not* divide the order of G , then G does not have a subgroup of order m .

Warning

The converse of Lagrange's Theorem is *false*.

Lagrange's Theorem does *not* assert that if m is a positive divisor of the order of a group G , then G has a subgroup of order m .

For example, the alternating group A_4 comprises the twelve even permutations in S_4 :

$$A_4 = \{e, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

The group A_4 has order 12, and the positive divisors of 12 are 1, 2, 3, 4, 6 and 12, so any subgroup of A_4 must have order 1, 2, 3, 4, 6 or 12. In fact, A_4 has subgroups of each of the orders 1, 2, 3, 4 and 12, as you are asked to show in the next exercise, but it has no subgroup of order 6. You are asked to show this later in this unit, in Exercise B144 in Subsection 2.6.

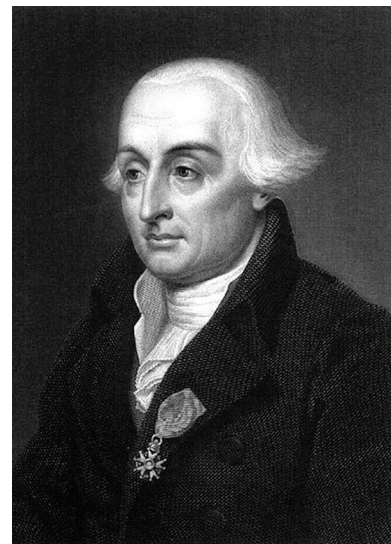
Exercise B133

Write down a subgroup of A_4 of each of the orders 1, 2, 3, 4 and 12.

Joseph-Louis Lagrange (1736–1813) was an Italian mathematician who spent his working life in Turin, Berlin and Paris. He made major contributions to mechanics, number theory and algebra. Today he is best known for his contributions to mechanics, where he transformed Newtonian mechanics into a branch of analysis, and won French Academy prizes for his work on celestial mechanics, with his memoir on the three-body problem being considered one of his most important works. (The *three-body problem* challenged mathematicians to develop a means of predicting how three neighbouring bodies in space, such as a star, a planet and a satellite, will move relative to each other.)

Lagrange's Theorem, which in modern mathematics is stated in terms of abstract groups, was obtained in the context of the theory of equations by Lagrange in 1771, a time when the concept of an abstract group had not yet been formulated. More specifically, Lagrange was trying to find an algebraic formula for the roots of a fifth degree polynomial equation and although he was unsuccessful (as Abel later showed he was bound to be), he was led to a theorem concerning the permutations of the roots of equations which, in essence, can be stated as follows: If a function of n variables is acted on by all $n!$ possible permutations of the variables and these permuted functions take only r distinct values, then r divides $n!$.

Lagrange's Theorem entered group theory with the work of both Gauss and Cauchy, each of whom proved it in particular cases. It was finally proved for any permutation group by Camille Jordan in 1861.



Joseph-Louis Lagrange
(grateful acknowledgement is made to the Royal College of Physicians for the image)

1.2 Corollaries of Lagrange's Theorem

Lagrange's Theorem is a cornerstone in the theory of finite groups. We now look at some of its useful corollaries.

Orders of group elements

Remember that the **order** of an element of a finite group G is the smallest positive integer n such that $x^n = e$. From Lagrange's Theorem we can deduce the following result.

Corollary B69 to Lagrange's Theorem

Let g be an element of a finite group G . Then the order of g divides the order of G .

Proof The order of g is the same as the order of the cyclic subgroup $\langle g \rangle$ generated by g , which divides the order of G by Lagrange's Theorem. ■

For example, in the group $S(\square)$, the element a (a quarter turn anticlockwise) has order 4, which is the same as the order of the cyclic subgroup generated by a :

$$\langle a \rangle = \{e, a, a^2, a^3\} = \{e, a, b, c\}.$$

This order is a divisor of 8, the order of $S(\square)$, as guaranteed by Lagrange's Theorem.

Exercise B134

Verify that the order of the group element divides the order of the group in each of the following cases.

- (a) The element $(1\ 2\ 3\ 4)$ of the group S_4 .
- (b) The element $(1\ 3\ 4)$ of the group S_4 .
- (c) The element 5 of the group $(\mathbb{Z}_9, +_9)$.
- (d) The element 6 of the group $(\mathbb{Z}_9, +_9)$.

Groups of prime order

We look next at groups of prime order. Lagrange's Theorem has the following corollary.

Corollary B70 to Lagrange's Theorem

Let G be a group of prime order. Then G is cyclic, and every element of G other than the identity element is a generator of G .

Proof Let the order of the group G be the prime number p , and let x be an element of G other than the identity element. Since p is prime, it follows from Lagrange's Theorem that the cyclic subgroup $\langle x \rangle$ generated by x has order 1 or p . However, only the identity element generates a cyclic subgroup of order 1, so the order of $\langle x \rangle$ is p , and hence $\langle x \rangle$ is the whole of G . Thus G is cyclic, and x is a generator of G . ■

Note that Corollary B70 tells us in particular that if a subgroup H of a group G has prime order, then H is a cyclic subgroup of G . This is because any subgroup of a group is itself a group.

Corollary B70 also gives us the following result.

Corollary B71 to Lagrange's Theorem

If G is a group of prime order p , then G is isomorphic to the cyclic group $(\mathbb{Z}_p, +_p)$.

Proof Let G be a group of prime order p . Then G is a cyclic group of order p , by Corollary B70. The group $(\mathbb{Z}_p, +_p)$ is also a cyclic group of order p (since $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n for any integer $n \geq 2$, by Theorem B37 in Unit B2). Any two cyclic groups of the same order are isomorphic (by Theorem B49 in Unit B2), so G is isomorphic to $(\mathbb{Z}_p, +_p)$. ■

The following corollary of Lagrange's Theorem tells us more about the structure of groups of prime order.

Corollary B72 to Lagrange's Theorem

If G is a group of prime order, then the only subgroups of G are the trivial subgroup and G itself.

Proof Let the order of G be the prime number p . Since p is prime, it follows from Lagrange's Theorem that any subgroup of G has order 1 or p . But the only subgroup of G of order 1 is the trivial subgroup $\{e\}$, and the only subgroup of G of order p is G itself. ■

An alternative way to prove Corollary B72 is to use Theorem B41 in Unit B2. This states that for any integer $n \geq 2$ the group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order q for each positive factor q of n , and no other subgroups. It follows that if p is prime, then the only subgroups of $(\mathbb{Z}_p, +_p)$ are the trivial subgroup and the whole group. By Corollary B71 (and Theorem B47 in Unit B2), the same must be true of any group of order p .

Exercise B135

Consider the group (G, \circ) of order 5 that is defined by the following Cayley table.

\circ	v	w	x	y	z
v	w	z	y	v	x
w	z	x	v	w	y
x	y	v	z	x	w
y	v	w	x	y	z
z	x	y	w	z	v

- Explain how you know that G is a cyclic group.
- Find the identity element of G and use the Cayley table to verify that all the other elements have order 5.
- Find an isomorphism ϕ that maps G to $(\mathbb{Z}_5, +_5)$.

Hint: Write down a generator of G and a generator of $(\mathbb{Z}_5, +_5)$, and then find an isomorphism by matching powers of generators (as in Strategy B6, near the end of Unit B2).

Exercise B136

- Let G be a group of order 14. Show that all the proper subgroups of G are cyclic. (Recall that a **proper** subgroup of a group G is a subgroup that is different from G itself.)
- More generally, let G be a group of order pq , where p and q are both prime. Show that all the proper subgroups of G are cyclic.

Corollaries B70 and B71 to Lagrange's Theorem can sometimes help us to determine how many isomorphism classes there are for groups of a given order.

In particular, Corollary B71 tells us that for each prime number p there is just one isomorphism class for groups of order p . In other words, all groups of a particular prime order p are isomorphic to each other.

The number of isomorphism classes for groups of order n for non-prime values of n is known for small values of n . For example, there are five isomorphism classes for groups of order 8 and fourteen isomorphism classes for groups of order 16. The isomorphism classes for groups of orders 1 to 8 are described in the next section. The problem of finding the isomorphism classes for groups of order n , and how many classes there are, becomes more difficult as n increases.

2 Groups of small order

In this section we will determine how many isomorphism classes there are for groups of orders 1 to 7. That is, we will determine how many different possible structures there are for groups of these orders. We will also look at the natures of these different structures. The isomorphism classes for groups of order 8 are also described here, without proof.

2.1 Some useful results

To enable us to determine isomorphism classes for small groups, we will use several theorems that you have met in this book, together with three further, more specialised, theorems that are stated and proved in this subsection.

Before you meet these three theorems it is useful for you to be introduced to a commonly used convention for notation in group theory. You met part of this convention in the last section: you saw that we often refer to an abstract group simply as G , without mentioning its binary operation. So far, however, we have continued to denote a composite of two elements x and y of an abstract group by $x \circ y$ (as we did, for example, in the proof of Lagrange's Theorem). This notation can become unwieldy when we deal with manipulations that involve a lot of composites of group elements, so for abstract groups we often drop the use of the symbol \circ in composites too. The complete convention is described below.

Notation convention for abstract groups

In discussions about abstract groups, we use the following notation and terminology where it will not cause confusion.

- We denote an abstract group simply by a single symbol such as G , without specifying a symbol for its binary operation.
- We denote a composite of two elements x and y of G simply by xy .

Warning: Unless the group is abelian, the composites xy and yx are not necessarily equal.

This convention makes the multiplicative notation that we have been using for abstract groups a little more concise. The features of multiplicative notation not mentioned in the box remain the same: for example, we continue to denote the inverse of an element x by x^{-1} , the composite of an element x with itself by x^2 , the identity element by e , and so on.

The notation described in the box above, which we will refer to as *concise multiplicative notation*, will be used in discussions and proofs involving abstract groups throughout the rest of this unit, and throughout Book E, except in some circumstances where it is clearer to revert to the notation that we used previously. It is usually quicker and easier to work with, once you are used to it. When you see results stated using this notation, you need to be able to convert them into notation that involves a symbol for the binary operation, and into additive notation, so you can apply them to particular groups. The next exercise should help you become familiar with the concise multiplicative notation.

Exercise B137

- (a) The following statements about elements x , y and z of a group G with identity element e are expressed using concise multiplicative notation, as described in the convention above. Write each of these statements using our previous standard notation for abstract groups, with the binary operation of G denoted by \circ . (One of the statements does not need to be changed.)
- (i) $ex = x$ (ii) $x^2x^3 = x^5$ (iii) $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$
 (iv) $x^0 = e$ (v) $xy = xz \implies y = z$
- (b) Write each of the statements in part (a) in additive notation, for a group $(G, +)$.

Now here is the first of the three new theorems that we will be using to help us determine isomorphism classes in this section. Its proof is written using concise multiplicative notation.

Theorem B73

Let G be a group in which each element except the identity has order 2. Then G is abelian.

Proof Let x and y be any elements of G . We have to show that $xy = yx$. Since xy is an element of G , it is either the identity element or has order 2, and hence

$$(xy)^2 = e,$$

that is,

$$e = xyxy.$$

Composing both sides of this equation on the left with x and on the right with y gives

$$xey = x^2yxy^2,$$

and hence, since x and y are either the identity element or have order 2,

$$xey = eyxe,$$

that is,

$$xy = yx.$$

Thus G is abelian. ■

Exercise B138

Construct an alternative proof of Theorem B73 by using the fact that if a group element g is either the identity element or has order 2 then it must be self-inverse, that is, it must have the property $g = g^{-1}$. Express your proof using concise multiplicative notation.

Hint: Let x and y be elements of the group G . Start by applying the fact mentioned above to the element xy .

Now here is the second of the three theorems that we will be using to help us determine isomorphism classes.

Theorem B74

Let G be a group of order greater than 2 in which each element except the identity has order 2. Then the order of G is a multiple of 4.

Proof

 We show that G has a subgroup of order 4, then apply Lagrange's Theorem. 

Since G has at least three elements, we can choose two distinct non-identity elements of G , say x and y . Since x and y have order 2, we have $x^2 = e$ and $y^2 = e$, and hence $x = x^{-1}$ and $y = y^{-1}$.

Let $z = xy$. Then z is distinct from e , x and y , because every other possibility leads to a contradiction:

$$z = e \text{ would imply } xy = e, \text{ and hence } y = x^{-1} = x;$$

$$z = x \text{ would imply } xy = x, \text{ and hence } y = e;$$

$$z = y \text{ would imply } xy = y, \text{ and hence } x = e.$$

We now show that $\{e, x, y, z\}$ is a subgroup of G . We start by determining the entries in the Cayley table for $\{e, x, y, z\}$. We already know that $x^2 = e$, $y^2 = e$ and $z^2 = e$, since $x, y, z \in G$. Also, by Theorem B73, the group G is abelian. Thus

$$yx = xy = z,$$

$$xz = x(xy) = x^2y = ey = y, \quad \text{so } zx = y \text{ also,}$$

$$yz = y(xy) = y(yx) = y^2x = ex = x, \quad \text{so } zy = x \text{ also.}$$

Hence the Cayley table is as follows.

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

We now check the three subgroup properties.

SG1 Closure Every element in the body of the table is in $\{e, x, y, z\}$, so $\{e, x, y, z\}$ is closed under the binary operation of G .

SG2 Identity The identity element e of G is in $\{e, x, y, z\}$.

SG3 Inverses All the elements of $\{e, x, y, z\}$ are self-inverse, so $\{e, x, y, z\}$ contains the inverse of each of its elements.

Thus $\{e, x, y, z\}$ is a subgroup of G . By Lagrange's Theorem, the order of this subgroup divides the order of G , so the order of G is a multiple of 4. ■

An example of a group that satisfies the conditions in Theorem B74 is $S(\square)$, the symmetry group of the rectangle, which has order 4.

The third of the three theorems in this subsection is as follows.

Theorem B75

Let G be a group of even order. Then G contains an element of order 2.

Proof The elements of G that are not self-inverse can be paired up with their inverses, so G has an even number of elements that are not self-inverse. Since G has even order, it follows that G also has an even number of elements that *are* self-inverse. The identity element is a self-inverse element, so there must be at least one further self-inverse element, say x . Since $x = x^{-1}$ it follows that $x^2 = e$, so x has order 1 or 2. But x is not the identity element, so it has order 2. ■

In fact, you can see from the proof of Theorem B75 that every group of even order has an odd number of elements of order 2.

In the remaining subsections of this section we will use the three theorems above to help us determine the isomorphism classes for groups of orders 1 to 7. (The classes for groups of order 8 are also described, without proof.) We will also use Lagrange's Theorem and some of its corollaries from Section 1, and the three theorems listed below, which you met earlier in this book.

- If two finite groups are isomorphic, then they have the same order. (Theorem B43 in Unit B2.)
- All finite cyclic groups of the same order are isomorphic. (Theorem B49 in Unit B2.)
- A group of order n that contains an element of order n is a cyclic group. (Theorem B34 in Unit B2.)

2.2 Groups of orders 1, 2, 3, 5 and 7

We now make a start on determining the isomorphism classes for groups of orders 1 to 7. It is straightforward to deal with the orders 1, 2, 3, 5 and 7.

Since every group contains an identity element, a group of order 1 consists of this element alone, and hence its Cayley table is simply the following, where e is the identity element.

$$\begin{array}{c|c} & e \\ \hline e & e \end{array}$$

So we can make the following observation.

Proposition B76 Isomorphism classes: order 1

There is only one isomorphism class for groups of order 1.

Examples of particular members of this isomorphism class are the groups

$$(\{0\}, +), (\{1\}, \times) \text{ and } S(F),$$

where F is any figure whose only symmetry is the identity symmetry.

Now let us consider groups of orders 2, 3, 5 and 7. All these orders are prime, so we can deal with them very easily by using Corollary B71 to Lagrange's Theorem, which states that a group of prime order p is isomorphic to the cyclic group $(\mathbb{Z}_p, +_p)$.

Proposition B77 Isomorphism classes: orders 2, 3, 5 and 7

For each prime p , there is only one isomorphism class for groups of order p . All the groups in this class are cyclic.

For example, all groups of order 2, such as $(\mathbb{Z}_2, +_2)$, (U_6, \times_6) and the group of direct symmetries of the rectangle, $S^+(\square)$, lie in the single isomorphism class for groups of order 2. That is, they are all isomorphic to each other.

Similarly, all groups of order 3, such as $(\mathbb{Z}_3, +_3)$, $(\{1, 4, 7\}, \times_9)$ and the group of direct symmetries of the triangle, $S^+(\triangle)$, lie in the single isomorphism class for groups of order 3.

Similar statements can be made for groups of orders 5 and 7.

Remember that we use the notation C_n to denote a general, abstract cyclic group of order n . So we can say that for any prime p , every group of order p is isomorphic to C_p . Remember also that every cyclic group is abelian.

2.3 Groups of order 4

In Subsection 4.2 of Unit B2 it was stated, without proof, that there are exactly two isomorphism classes for groups of order 4. We can now prove this fact.

Suppose that G is a group of order 4. By Corollary B69 to Lagrange's Theorem, the order of each element of G divides 4, so each element of G has order 1, 2 or 4. We will consider separately the following two possibilities:

- G has an element of order 4
- G has no element of order 4.

G has an element of order 4

If G has an element of order 4, then G is a cyclic group, isomorphic to C_4 . The pattern of the Cayley table of this group is shown in Figure 3.

Examples of cyclic groups of order 4 include $(\mathbb{Z}_4, +_4)$, $(\mathbb{Z}_5^*, \times_5)$ and the group of direct symmetries of the square, $S^+(\square)$.

G has no element of order 4

Now consider the other possibility, that G does not have an element of order 4. Only the identity element has order 1, so the other three elements of G have order 2. If we let two of these elements be x and y , and we let $z = xy$, then by exactly the same argument as in the proof of Theorem B74 we can deduce that z is distinct from e , x and y , and that the Cayley table for $\{e, x, y, z\}$ is as follows.

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

Since G has only four elements, this is the Cayley table of G . The table has the pattern of the Klein four-group V , shown in Figure 4, which you met in Subsection 4.2 of Unit B2. So G is isomorphic to the Klein four-group. In particular, G is abelian.

Examples of groups of order 4 isomorphic to the Klein four-group V include (U_8, \times_8) and the symmetry group of the rectangle, $S(\square)$.

We have established the following result.



Figure 3 The pattern of the Cayley table of C_4



Figure 4 The pattern of the Cayley table of the Klein four-group

Proposition B78 Isomorphism classes: order 4

There are two isomorphism classes for groups of order 4:

- one contains the cyclic group C_4
- the other contains the Klein four-group V .

All groups of order 4 are abelian.

Given a group G of order 4, we can determine the isomorphism class to which it belongs by looking at the orders of its elements, as follows.

- If there are only two self-inverse elements (or, alternatively, if there is an element of order 4 – there would be two such elements), then $G \cong C_4$.
- If all elements are self-inverse (or, alternatively, if there is no element of order 4), then $G \cong V$.

Remember that the symbol \cong means ‘is isomorphic to’.

Recall that you can see immediately from a group table whether a particular element x is self-inverse, by checking whether the cell in the row labelled x and column labelled x contains the identity element, as illustrated in Figure 5.

Exercise B139

Each of the following sets is a subgroup of the symmetric group S_6 . In each case, determine whether the subgroup is isomorphic to C_4 or to V .

- $\{e, (1\ 3), (2\ 5), (1\ 3)(2\ 5)\}$
- $\{e, (2\ 3\ 4\ 6), (2\ 4)(3\ 6), (2\ 6\ 4\ 3)\}$

Notice from the Cayley table for $\{e, x, y, z\}$ above that in a group isomorphic to the Klein four-group V , the composite of any pair of distinct non-identity elements is the third non-identity element. That is, if the three non-identity elements are x, y and z , then $xy = z$, $xz = y$ and $yz = x$. It is useful to remember this fact.

2.4 Groups of order 6

In Subsection 4.2 of Unit B2 it was stated, without proof, that there are exactly two isomorphism classes for groups of order 6. We now prove this result.

Suppose that G is a group of order 6. Then each element of G has order 1, 2, 3 or 6. We will consider separately the following two possibilities:

- G has an element of order 6
- G has no element of order 6.

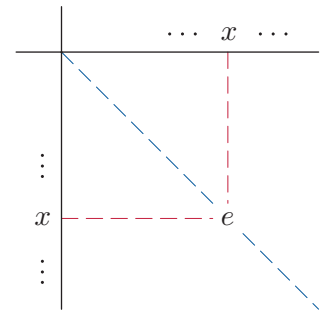


Figure 5 A self-inverse element x

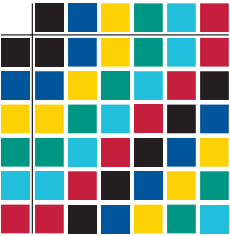


Figure 6 The pattern of the Cayley table of C_6

G has an element of order 6

If G has an element of order 6, then G is a cyclic group, isomorphic to C_6 . The pattern of the Cayley table of this group is shown in Figure 6.

Examples of cyclic groups of order 6 include $(\mathbb{Z}_6, +_6)$ and $(\mathbb{Z}_7^*, \times_7)$.

G has no element of order 6

Now consider the other possibility, that G does not contain an element of order 6. In this case each non-identity element of G has order 2 or 3. By Theorem B75, since G has even order, it contains an element of order 2, say g . However, not all the non-identity elements of G have order 2, by Theorem B74, since the order of G is 6, which is not a multiple of 4. So G also contains an element of order 3, say h .

Let H be the cyclic subgroup generated by h :

$$H = \langle h \rangle = \{e, h, h^2\}.$$

The element g does not lie in H , because H has order 3 and so its elements have order 1 or 3 by Corollary B69 to Lagrange's Theorem. Hence, by the argument in the proof of Lagrange's Theorem, the following array is an arrangement of the elements of G :

$$\begin{array}{ccc} e & h & h^2 \\ g & gh & gh^2. \end{array}$$

(Remember that we are using concise multiplicative notation, so we write gh rather than $g \circ h$, and gh^2 rather than $g \circ h^2$.)

Thus the six distinct elements of G are

$$e, h, h^2, g, gh, gh^2.$$

We now construct a Cayley table for G . We can construct some of it directly by using the information that we have so far, as follows.

	e	h	h^2	g	gh	gh^2
e	e	h	h^2	g	gh	gh^2
h	h	h^2	e			
h^2	h^2	e	h			
g	g	gh	gh^2	e	h	h^2
gh	gh	gh^2	g			
gh^2	gh^2	g	gh			

To make further progress we need to evaluate the composite hg , which must be one of the six elements e, h, h^2, g, gh, gh^2 . It cannot be h, h^2 or e since they already appear in the same row, and it cannot be g since it already appears in the same column. That leaves the possibilities gh and gh^2 .

We use proof by contradiction to show that $hg \neq gh$. If $hg = gh$, then we would have

$$\begin{aligned} hg &= gh \neq e, \\ (hg)^2 &= (hg)(hg) = (hg)(gh) = hg^2h = heh = h^2 \neq e, \\ (hg)^3 &= (hg)^2(hg) = h^2(hg) = h^3g = eg = g \neq e, \end{aligned}$$

which would tell us that the order of hg is not 1, 2 nor 3, and hence must be 6 (since the order of a group element divides the order of the group). But this would contradict the fact that G has no element of order 6. Therefore we must have

$$hg = gh^2.$$

We can enter this in the Cayley table, and we can then fill in the rest of the top right quarter of the table using only the fact that each group element must occur exactly once in each row and each column. However, we need to calculate one more entry before we can do the same for the bottom right quarter. Since $hg = gh^2$, we have

$$(gh)g = g(hg) = g(gh^2) = g^2h^2 = eh^2 = h^2.$$

If we fill in this entry and complete the rest of the table using the fact that each group element must occur exactly once in each row and each column, then we obtain the following table.

	e	h	h^2	g	gh	gh^2
e	e	h	h^2	g	gh	gh^2
h	h	h^2	e	gh^2	g	gh
h^2	h^2	e	h	gh	gh^2	g
g	g	gh	gh^2	e	h	h^2
gh	gh	gh^2	g	h^2	e	h
gh^2	gh^2	g	gh	h	h^2	e

This table has the pattern shown in Figure 7, which is the same as the pattern of the Cayley tables of the groups $S(\triangle)$ and S_3 , shown below. This pattern is not symmetric with respect to the main diagonal, so these groups are not abelian.

\circ	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$S(\triangle)$

\circ	e	(123)	(132)	(23)	(13)	(12)
e	e	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	e	(12)	(23)	(13)
(132)	(132)	e	(123)	(13)	(12)	(23)
(23)	(23)	(13)	(12)	e	(123)	(132)
(13)	(13)	(12)	(23)	(132)	e	(123)
(12)	(12)	(23)	(13)	(123)	(132)	e

S_3

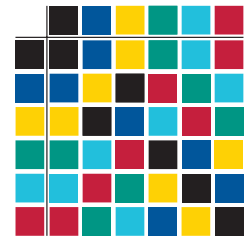


Figure 7 The pattern of the Cayley tables of $S(\triangle)$ and S_3

So we have established the following result.

Proposition B79 Isomorphism classes: order 6

There are two isomorphism classes of groups of order 6:

- one contains the cyclic group C_6
- the other contains the non-abelian group $S(\triangle)$.

Given a group G of order 6, we can determine the isomorphism class to which it belongs by using the fact that one class contains abelian groups and the other class contains non-abelian groups, as follows.

- If the group table is symmetric with respect to the main diagonal, then $G \cong C_6$.
- If the group table is not symmetric with respect to the main diagonal, then $G \cong S(\triangle)$.

Exercise B140

Find each of the following in the symmetric group S_6 .

- A subgroup isomorphic to C_6 .
- A subgroup isomorphic to $S(\triangle)$.

The group $S(\triangle)$ is known as the *dihedral group* of order 6.

More generally, for each integer $n \geq 3$, the symmetry group of the regular polygon with n edges is called the **dihedral group** of order $2n$. For example, $S(\square)$ is the dihedral group of order 8, $S(\diamond)$ is the dihedral group of order 10, and so on. The dihedral group of order $2n$ is usually denoted by D_n (or, in some texts, by D_{2n}), but this notation is not used in this module.

2.5 Groups of order 8

We now turn to groups of order 8. Suppose that G is a group of order 8. Then each element of G has order 1, 2, 4 or 8. So every group of order 8 satisfies exactly one of the following three possibilities:

- G has an element of order 8
- G has no element of order 8, but has an element of order 4
- each element of G except e has order 2.

These possibilities are discussed below (in a slightly different order), with the proofs omitted.

G has an element of order 8

If G has an element of order 8, then G is a cyclic group, isomorphic to C_8 . Thus G is abelian.

Such a group G comprises the identity, four elements of order 8, two elements of order 4 and one element of order 2.

An example of a cyclic group of order 8 is $(\mathbb{Z}_8, +_8)$. The orders of the elements in this group are as follows.

Element	0	1	2	3	4	5	6	7
Order	1	8	4	8	2	8	4	8

Each element of G except e has order 2

Here G is a group comprising the identity and seven elements of order 2, so, by Theorem B73, it is abelian. It can be shown that all such groups are isomorphic to each other.

An example of a group with this structure is the symmetry group of a cuboid with no square faces. You met this group in Exercise B34 in Unit B1. We can denote it by $S(\text{cuboid})$. It contains the identity symmetry, three rotations through π as shown in Figure 8, three reflections in planes halfway between opposite faces, and one further indirect symmetry, which maps each point of the cuboid to the ‘opposite’ point, that is, to the point that is reached if a line is drawn from the original point to the centre of the cuboid and then extended by the same distance again. You can think of this fourth indirect symmetry as ‘reflection in the central point of the cuboid’.

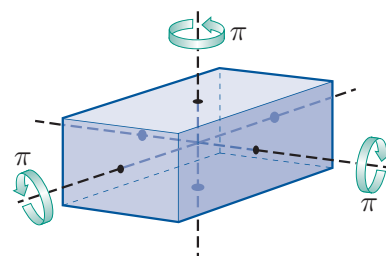


Figure 8 A cuboid and its three non-identity rotational symmetries

G has no element of order 8, but has an element of order 4

In this case, each non-identity element of G has order 2 or 4. Using an approach similar to that used for groups of order 6, we can show that there are three non-isomorphic groups of this type, as follows.

- A non-cyclic abelian group comprising the identity, four elements of order 4 and three elements of order 2. The group (U_{15}, \times_{15}) , for example, has this structure, as you are asked to show in Exercise B141 below.
- A non-abelian group comprising the identity, two elements of order 4 and five elements of order 2. The group $S(\square)$, that is, the dihedral group of order 8, has this structure. The non-identity elements of $S(\square)$ are shown in Figure 9, and the orders of the elements are as follows.

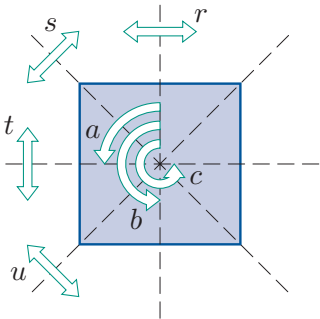


Figure 9
 $S(\square)$

Element	e	a	b	c	r	s	t	u
Order	1	4	2	4	2	2	2	2

- A non-abelian group comprising the identity, six elements of order 4 and one element of order 2. The standard example of such a group is the **quaternion group** of order 8, denoted by Q_8 . (The blue box at the end of this subsection gives some of the history behind its name.) The elements of this group are usually denoted by

$$1, -1, i, -i, j, -j, k, -k,$$

where i, j and k are simply symbols, and $-i, -j$ and $-k$ denote the composites $(-1)i, (-1)j$ and $(-1)k$. The Cayley table for Q_8 is shown below. Notice that $i^2 = j^2 = k^2 = -1$. It is straightforward to check that the Cayley table satisfies group axioms G1 (closure), G3 (identity) and G4 (inverses), and it can be shown that it also satisfies axiom G2 (associativity).

\times	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

The orders of the elements of Q_8 are as follows.

Element	1	-1	i	$-i$	j	$-j$	k	$-k$
Order	1	2	4	4	4	4	4	4

Exercise B141

Show that (U_{15}, \times_{15}) is an abelian group of order 8 that has four elements of order 4 and three elements of order 2.

Exercise B142

Use the Cayley table of the quaternion group Q_8 to show that the elements i and $-i$ of this group both have order 4.

(You can denote a composite of elements x and y of Q_8 by xy , as the binary operation of Q_8 may be thought of as a type of multiplication. Remember though that xy and yx may not be equal.)

The discussion above about groups of order 8 is summarised in the following proposition.

Proposition B80 Isomorphism classes: order 8

There are five isomorphism classes for groups of order 8, as follows.

Class	Abelian/ non-abelian	Numbers of elements of				Example
		order 1	order 2	order 4	order 8	
1	abelian	1	1	2	4	$(\mathbb{Z}_8, +_8)$
2	abelian	1	7	0	0	$S(\text{cuboid})$
3	abelian	1	3	4	0	(U_{15}, \times_{15})
4	non-abelian	1	5	2	0	$S(\square)$
5	non-abelian	1	1	6	0	Q_8

This gives us the following strategy.

Strategy B14

To determine the isomorphism class of a group of order 8, determine whether the group is abelian and find the number of elements of order 2. Then use the table in Proposition B80.

You can count how many elements of order 2 there are in a finite group by looking at its Cayley table: the number of elements of order 2 is one less than the number of self-inverse elements, because the self-inverse elements are the identity element and the elements of order 2. Remember also that a finite group is abelian if and only if its Cayley table is symmetric with respect to the main diagonal.

Exercise B143

Each of the following Cayley tables is the group table of a group of order 8. In each case, use Strategy B14 to determine the isomorphism class to which the group belongs, and hence state a standard group from Proposition B80 to which the group is isomorphic.

(a)	<table><tr><th>\circ</th><th>e</th><th>a</th><th>b</th><th>c</th><th>d</th><th>f</th><th>g</th><th>h</th></tr><tr><th>e</th><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td></tr><tr><th>a</th><td>a</td><td>e</td><td>c</td><td>b</td><td>f</td><td>d</td><td>h</td><td>g</td></tr><tr><th>b</th><td>b</td><td>c</td><td>e</td><td>a</td><td>g</td><td>h</td><td>d</td><td>f</td></tr><tr><th>c</th><td>c</td><td>b</td><td>a</td><td>e</td><td>h</td><td>g</td><td>f</td><td>d</td></tr><tr><th>d</th><td>d</td><td>f</td><td>g</td><td>h</td><td>e</td><td>a</td><td>b</td><td>c</td></tr><tr><th>f</th><td>f</td><td>d</td><td>h</td><td>g</td><td>a</td><td>e</td><td>c</td><td>b</td></tr><tr><th>g</th><td>g</td><td>h</td><td>d</td><td>f</td><td>b</td><td>c</td><td>e</td><td>a</td></tr><tr><th>h</th><td>h</td><td>g</td><td>f</td><td>d</td><td>c</td><td>b</td><td>a</td><td>e</td></tr></table>	\circ	e	a	b	c	d	f	g	h	e	e	a	b	c	d	f	g	h	a	a	e	c	b	f	d	h	g	b	b	c	e	a	g	h	d	f	c	c	b	a	e	h	g	f	d	d	d	f	g	h	e	a	b	c	f	f	d	h	g	a	e	c	b	g	g	h	d	f	b	c	e	a	h	h	g	f	d	c	b	a	e	(b)	<table><tr><th>\circ</th><th>e</th><th>a</th><th>b</th><th>c</th><th>d</th><th>f</th><th>g</th><th>h</th></tr><tr><th>e</th><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td></tr><tr><th>a</th><td>a</td><td>b</td><td>c</td><td>e</td><td>f</td><td>g</td><td>h</td><td>d</td></tr><tr><th>b</th><td>b</td><td>c</td><td>e</td><td>a</td><td>g</td><td>h</td><td>d</td><td>f</td></tr><tr><th>c</th><td>c</td><td>e</td><td>a</td><td>b</td><td>h</td><td>d</td><td>f</td><td>g</td></tr><tr><th>d</th><td>d</td><td>f</td><td>g</td><td>h</td><td>e</td><td>a</td><td>b</td><td>c</td></tr><tr><th>f</th><td>f</td><td>g</td><td>h</td><td>d</td><td>a</td><td>b</td><td>c</td><td>e</td></tr><tr><th>g</th><td>g</td><td>h</td><td>d</td><td>f</td><td>b</td><td>c</td><td>e</td><td>a</td></tr><tr><th>h</th><td>h</td><td>d</td><td>f</td><td>g</td><td>c</td><td>e</td><td>a</td><td>b</td></tr></table>	\circ	e	a	b	c	d	f	g	h	e	e	a	b	c	d	f	g	h	a	a	b	c	e	f	g	h	d	b	b	c	e	a	g	h	d	f	c	c	e	a	b	h	d	f	g	d	d	f	g	h	e	a	b	c	f	f	g	h	d	a	b	c	e	g	g	h	d	f	b	c	e	a	h	h	d	f	g	c	e	a	b
\circ	e	a	b	c	d	f	g	h																																																																																																																																																													
e	e	a	b	c	d	f	g	h																																																																																																																																																													
a	a	e	c	b	f	d	h	g																																																																																																																																																													
b	b	c	e	a	g	h	d	f																																																																																																																																																													
c	c	b	a	e	h	g	f	d																																																																																																																																																													
d	d	f	g	h	e	a	b	c																																																																																																																																																													
f	f	d	h	g	a	e	c	b																																																																																																																																																													
g	g	h	d	f	b	c	e	a																																																																																																																																																													
h	h	g	f	d	c	b	a	e																																																																																																																																																													
\circ	e	a	b	c	d	f	g	h																																																																																																																																																													
e	e	a	b	c	d	f	g	h																																																																																																																																																													
a	a	b	c	e	f	g	h	d																																																																																																																																																													
b	b	c	e	a	g	h	d	f																																																																																																																																																													
c	c	e	a	b	h	d	f	g																																																																																																																																																													
d	d	f	g	h	e	a	b	c																																																																																																																																																													
f	f	g	h	d	a	b	c	e																																																																																																																																																													
g	g	h	d	f	b	c	e	a																																																																																																																																																													
h	h	d	f	g	c	e	a	b																																																																																																																																																													
(c)	<table><tr><th>\circ</th><th>e</th><th>a</th><th>b</th><th>c</th><th>d</th><th>f</th><th>g</th><th>h</th></tr><tr><th>e</th><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td></tr><tr><th>a</th><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td><td>e</td></tr><tr><th>b</th><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td><td>e</td><td>a</td></tr><tr><th>c</th><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td><td>e</td><td>a</td><td>b</td></tr><tr><th>d</th><td>d</td><td>f</td><td>g</td><td>h</td><td>e</td><td>a</td><td>b</td><td>c</td></tr><tr><th>f</th><td>f</td><td>g</td><td>h</td><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td></tr><tr><th>g</th><td>g</td><td>h</td><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td></tr><tr><th>h</th><td>h</td><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td></tr></table>	\circ	e	a	b	c	d	f	g	h	e	e	a	b	c	d	f	g	h	a	a	b	c	d	f	g	h	e	b	b	c	d	f	g	h	e	a	c	c	d	f	g	h	e	a	b	d	d	f	g	h	e	a	b	c	f	f	g	h	e	a	b	c	d	g	g	h	e	a	b	c	d	f	h	h	e	a	b	c	d	f	g	(d)	<table><tr><th>\circ</th><th>e</th><th>a</th><th>b</th><th>c</th><th>d</th><th>f</th><th>g</th><th>h</th></tr><tr><th>e</th><td>e</td><td>a</td><td>b</td><td>c</td><td>d</td><td>f</td><td>g</td><td>h</td></tr><tr><th>a</th><td>a</td><td>b</td><td>c</td><td>e</td><td>f</td><td>g</td><td>h</td><td>d</td></tr><tr><th>b</th><td>b</td><td>c</td><td>e</td><td>a</td><td>g</td><td>h</td><td>d</td><td>f</td></tr><tr><th>c</th><td>c</td><td>e</td><td>a</td><td>b</td><td>h</td><td>d</td><td>f</td><td>g</td></tr><tr><th>d</th><td>d</td><td>h</td><td>g</td><td>f</td><td>b</td><td>a</td><td>e</td><td>c</td></tr><tr><th>f</th><td>f</td><td>d</td><td>h</td><td>g</td><td>c</td><td>b</td><td>a</td><td>e</td></tr><tr><th>g</th><td>g</td><td>f</td><td>d</td><td>h</td><td>e</td><td>c</td><td>b</td><td>a</td></tr><tr><th>h</th><td>h</td><td>g</td><td>f</td><td>d</td><td>a</td><td>e</td><td>c</td><td>b</td></tr></table>	\circ	e	a	b	c	d	f	g	h	e	e	a	b	c	d	f	g	h	a	a	b	c	e	f	g	h	d	b	b	c	e	a	g	h	d	f	c	c	e	a	b	h	d	f	g	d	d	h	g	f	b	a	e	c	f	f	d	h	g	c	b	a	e	g	g	f	d	h	e	c	b	a	h	h	g	f	d	a	e	c	b
\circ	e	a	b	c	d	f	g	h																																																																																																																																																													
e	e	a	b	c	d	f	g	h																																																																																																																																																													
a	a	b	c	d	f	g	h	e																																																																																																																																																													
b	b	c	d	f	g	h	e	a																																																																																																																																																													
c	c	d	f	g	h	e	a	b																																																																																																																																																													
d	d	f	g	h	e	a	b	c																																																																																																																																																													
f	f	g	h	e	a	b	c	d																																																																																																																																																													
g	g	h	e	a	b	c	d	f																																																																																																																																																													
h	h	e	a	b	c	d	f	g																																																																																																																																																													
\circ	e	a	b	c	d	f	g	h																																																																																																																																																													
e	e	a	b	c	d	f	g	h																																																																																																																																																													
a	a	b	c	e	f	g	h	d																																																																																																																																																													
b	b	c	e	a	g	h	d	f																																																																																																																																																													
c	c	e	a	b	h	d	f	g																																																																																																																																																													
d	d	h	g	f	b	a	e	c																																																																																																																																																													
f	f	d	h	g	c	b	a	e																																																																																																																																																													
g	g	f	d	h	e	c	b	a																																																																																																																																																													
h	h	g	f	d	a	e	c	b																																																																																																																																																													

The quaternions

In 1843 the Irish mathematician William Rowan Hamilton (1805–1865) published a paper in which he carefully explained how complex numbers can be regarded as ordered pairs of real numbers; specifically $a + ib = (a, b)$. Complex numbers are a convenient notation for pairs, but space is three-dimensional, and his paper sparked a search for a similar notation for triples. What was required was a way of adding two triples so as to obtain a third, and multiplying two triples so as to obtain a third, in such a way that subtraction and division are also possible. The search for triples with the required properties always failed and later it was proved that no such algebra of triples can exist. But in 1843 Hamilton surprised himself by discovering an algebra of quadruples in which quadruples can be added, subtracted, multiplied and (if non-zero) divided.



William Rowan Hamilton

Hamilton introduced three symbols i , j and k and gave them simple but unexpected rules for their multiplication:

$$\begin{aligned}i^2 &= j^2 = k^2 = -1, \\ij &= k, \quad jk = i, \quad ki = j, \\ij &= -ji, \quad jk = -kj, \quad ki = -ik.\end{aligned}$$

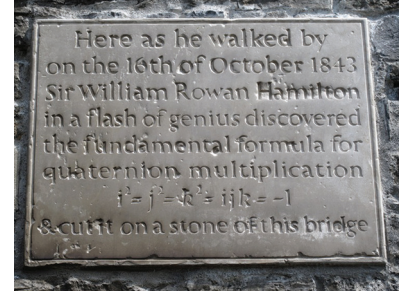
The third rule was a shock to almost everyone who saw it – everyone who had been looking for an algebra of triples up to this point had assumed that multiplication must be commutative. Hamilton then wrote quadruples as expressions of the form $w + xi + yj + zk$, where x , y , z , and w are real numbers. He called these quadruples quaternions, and studied the algebra that resulted.

Hamilton left an account of his discovery in the form of a letter to his son, Archibald, written almost twenty years later. In it he famously described how he could not ‘resist the impulse – unphilosophical as it may have been – to cut with a knife on a stone of Brougham Bridge, as we passed it, the fundamental formula with the symbols, i , j , k ; namely

$$i^2 = j^2 = k^2 = -1,$$

which contains the Solution of the Problem, but of course, as an inscription, has long since mouldered away.’ There is now a stone plaque commemorating Hamilton’s discovery set into the side of the bridge.

You saw earlier (in Subsection 3.4 of Unit B1 and Subsection 1.2 of Unit B2, respectively) that the complex numbers form an infinite group under multiplication when the element $0 = 0 + 0i$ is excluded, and $\{1, -1, i, -i\}$ is a subgroup of this infinite group. In a similar way, the quaternions form an infinite group under multiplication when the element $0 = 0 + 0i + 0j + 0k$ is excluded, and the quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is a subgroup of this infinite group.



The plaque on Brougham Bridge (usually known as Broome Bridge) in Dublin. It reads: Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ & cut it on a stone of this bridge

2.6 Summary of isomorphism classes for groups of orders 1 to 8

Table 5 summarises the results of Subsections 2.2 to 2.5. It lists the isomorphism classes for groups of orders 1 to 8, and places some of the groups that you have met in their classes.

Table 5 Isomorphism classes for groups of orders 1 to 8

Order	Standard group(s)	Properties	Further examples
1	C_1	cyclic	$(\{0\}, +), (\{1\}, \times)$
2	$C_2, (\mathbb{Z}_2, +_2)$	cyclic	$S^+(\square), (\mathbb{Z}_3^*, \times_3)$
3	$C_3, (\mathbb{Z}_3, +_3)$	cyclic	$S^+(\triangle), (\{0, 4, 8\}, +_{12}),$ $(\{1, 4, 7\}, \times_9)$
4	$C_4, (\mathbb{Z}_4, +_4)$	cyclic	$(\mathbb{Z}_5^*, \times_5), S^+(\square), S(\frac{\circ}{\circ}),$ $(\{0, 3, 6, 9\}, +_{12}),$ $(\{1, -1, i, -i\}, \times)$
	$V, S(\square)$	abelian, non-cyclic	$(U_8, \times_8), (U_{12}, \times_{12}),$ $(\{1, 7, 9, 15\}, \times_{16}),$ $(\{1, 9, 11, 19\}, \times_{20})$
5	$C_5, (\mathbb{Z}_5, +_5)$	cyclic	$S^+(\diamond)$
6	$C_6, (\mathbb{Z}_6, +_6)$	cyclic	$S^+(\diamond), (\mathbb{Z}_7^*, \times_7), (U_9, \times_9),$ $(\{0, 2, 4, 6, 8, 10\}, +_{12}),$ (U_{14}, \times_{14})
	$S(\triangle)$	non-abelian	$S_3, \{e, (2\,3), (2\,4), (3\,4),$ $(2\,3\,4), (2\,4\,3)\}$
7	$C_7, (\mathbb{Z}_7, +_7)$	cyclic	$S^+(\text{heptagon})$
8	$C_8, (\mathbb{Z}_8, +_8)$	cyclic	$S^+(\text{octagon})$
	$S(\text{cuboid})$	abelian	
	(U_{15}, \times_{15})	abelian	(U_{20}, \times_{20})
	$S(\square)$	non-abelian	
	Q_8	non-abelian	

In the next exercise you can use what you have learned about the isomorphism classes for small groups to show that the alternating group A_4 , a group of order 12, has no subgroup of order 6, as mentioned in Subsection 1.1. This shows that although Lagrange's Theorem tells us the *possible* orders of a subgroup of a group, there may not be a subgroup of each of these possible orders.

This exercise is quite challenging: it needs puzzling out. Try it for a few minutes, and if you are not making progress then look at the hint given at the start of the solution to the exercise. (Try not to look at the solution itself when you do so!)

Exercise B144

The alternating group A_4 is given by

$$A_4 = \{e, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), \\ (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3), \\ (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Use a contradiction argument to show that A_4 has no subgroup of order 6.

3 Theorems and proofs in group theory

Throughout this book you have met many theorems and proofs, and you have been asked to produce some proofs of your own. In this section we will look again at the different ways in which theorems can be stated, in the context of the group theory that you have met, and we will revisit some of the simpler proofs in group theory that you have seen, and prove a few further results. This work should strengthen your ability to apply theorems correctly, understand proofs and produce your own proofs. These skills will be important in the remainder of the module.

3.1 Statements of theorems

Before you can prove, or indeed apply, a theorem, you need to be completely clear about what it actually claims. Any theorem can be expressed in many different ways using the elements of mathematical language that you met in Unit A3 *Mathematical language and proof*, and you will see theorems expressed in a variety of different ways throughout this module. In general, mathematicians aim to express each theorem as clearly and concisely as possible, using whatever language seems to suit that particular theorem. In this subsection you will practise interpreting theorems correctly, no matter how they are expressed.

Consider the following theorem, which you met in Unit B1. It is headed 'Proposition' rather than 'Theorem' because this word is often used for theorems that are 'less important' in some way (for example, they might be quick and straightforward to prove).

Proposition B11

In any group, the identity element is unique.

This theorem is expressed as a *universal statement*: it says that a particular property (a unique identity element) holds for *every* group. The word 'any' has been used, but it could just as well have been 'every'.

Another way in which the same theorem can be expressed is as follows.

Proposition B11 (version 2)

If G is a group, then the identity element of G is unique.

Here the theorem is stated in the form 'If P , then Q ', where P and Q are statements. That is, it is expressed as an **implication**. Remember from Unit A3 that when you see a theorem expressed as an implication, it is to be interpreted as a universal statement, with the 'For all ...' part omitted but understood implicitly. For example, the statement above really means

For all G , if G is a group, then the identity element of G is unique.

Many theorems can be expressed as implications in this way.

In Unit A3 you saw that the statements P and Q in an implication 'If P then Q ' are called the **hypothesis** and the **conclusion** of the implication, respectively. For Proposition B11, the hypothesis is ' G is a group' and the conclusion is 'the identity element of G is unique'.

There are various different ways to express a theorem as an implication, because, as you saw in Unit A3, an implication 'If P , then Q ' can be expressed in various ways, such as those below.

Ways to express the implication 'If P , then Q '

- P implies Q
- $P \implies Q$
- P is sufficient for Q
- P only if Q
- Q whenever P
- Q follows from P
- Q is necessary for P
- Q provided that P

For instance, here are two alternative ways to express Proposition B11, by rewriting the implication in version 2 in different ways.

Proposition B11 (version 3)

The identity element of G is unique whenever G is a group.

Proposition B11 (version 4)

G is a group only if the identity element of G is unique.

Versions 3 and 4 of Proposition B11 would probably not be used in practice, because they do not read naturally and are less easy to understand than versions 1 and 2. In particular, when the phrase ‘only if’ appears in a theorem, it is usually part of the phrase ‘if and only if’, which is discussed later in this subsection.

Finally, here is one more way in which Proposition B11 can be expressed.

Proposition B11 (version 5)

Let G be a group. Then the identity element of G is unique.

Here the theorem is stated in the form ‘Let P . Then Q ’, where P and Q are statements. This is a very common way to express a theorem that could also be expressed as an implication ‘If P , then Q ’. It is particularly useful when the statements P and Q are themselves quite complicated. The sentence of the form ‘Let P ’ sets up a condition, P , that we are to assume holds for the remainder of the statement of the theorem. Then the sentence of the form ‘Then Q ’ asserts that Q always holds under this condition. We still refer to the statements P and Q as the hypothesis and the conclusion, respectively, of the theorem. There are of course alternative ways to express the sentences of the form ‘Let P ’ and ‘Then Q ’: a common alternative to ‘Let P ’ is ‘Suppose P ’.

Worked Exercise B48

The following theorem is from Subsection 2.2 of Unit B2. Rephrase it in the form 'If ..., then ...', and state its hypothesis and conclusion.

Theorem B29

Let x be an element of a finite group G . Then x has finite order.

Solution

The theorem can be rephrased as follows.

If x is an element of a finite group G , then x has finite order.

The hypothesis is

x is an element of a finite group G .

The conclusion is

x has finite order.

The theorem in the next exercise is headed 'Corollary'. Recall that a *corollary* is a theorem that follows from another theorem by a short additional argument.

Exercise B145

The following theorem is from Subsection 3.4 of Unit B1.

Corollary B10

If p is a prime number, then $(\mathbb{Z}_p^*, \times_p)$ is a group.

- (a) State the hypothesis and conclusion of this theorem.
- (b) Rephrase the theorem in each of the following forms.
 - (i) Let Then
 - (ii) ... whenever
 - (iii) ... provided that
 - (iv) ... only if
- (c) Which of your answers to part (b) do you think would be good ways to state the theorem?

If the hypothesis P of a theorem is of the form ‘ P_1 and P_2 and ... and P_n ’ (it may not be phrased exactly like this, of course), then we usually call the individual statements P_1, P_2, \dots, P_n the **hypotheses** of the theorem. Similarly, if the conclusion Q is of the form ‘ Q_1 and Q_2 and ... and Q_n ’, then we usually call the individual statements Q_1, Q_2, \dots, Q_n the **conclusions** of the theorem.

No matter how a theorem is phrased, it is important that you can recognise all of its hypotheses and all of its conclusions, and that you do not mix them up. When you apply the theorem, you must make sure that all the hypotheses are satisfied before you can deduce the conclusion(s).

Worked Exercise B49

The following theorem is from Subsection 2.1 of Unit B2. (It is restated here using concise multiplicative notation.) State its hypotheses and conclusions.

Theorem B27 Index laws

Let x be an element of a group G , and let m and n be integers. The following index laws hold.

- (a) $x^m x^n = x^{m+n}$
- (b) $(x^m)^n = x^{mn}$
- (c) $(x^n)^{-1} = x^{-n} = (x^{-1})^n$

Solution

The hypotheses are

- x is an element of a group G ,
- m and n are integers.

The conclusions are

- $x^m x^n = x^{m+n}$,
- $(x^m)^n = x^{mn}$,
- $(x^n)^{-1} = x^{-n} = (x^{-1})^n$.

Notice that the theorem in Worked Exercise B49 has the ‘Let ... Then ...’ form, but with the word ‘Then’ omitted and treated as understood.

Exercise B146

The following theorem is from Subsection 3.3 of Unit B2.

Theorem B37

For each integer $n \geq 2$, the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n . It is generated by the integer 1.

- (a) Rewrite the theorem in the form 'If ..., then ...'.
- (b) State the hypothesis (or hypotheses) and conclusion (or conclusions) of the theorem.

The next exercise asks you to state the *converse* of a theorem. Remember from Unit A3 that the **converse** of the implication 'If P then Q ' is the implication 'If Q then P '. The converse of a true implication may or may not be true.

Exercise B147

The following theorem is from Subsection 3.2 of Unit B2.

Theorem B35

Every cyclic group is abelian.

- (a) Rewrite the theorem in the form 'If ..., then ...'.
(You might find it helpful to introduce a symbol G for the group, as was done in version 2 of Proposition B11, discussed near the start of this subsection.)
- (b) State the converse of the theorem.
- (c) Is the converse true? Briefly justify your answer.

The solution to Exercise B147 illustrates another point that it is useful to keep in mind when you work with theorems and proofs. As you have seen, we aim to write mathematical statements in a way that is as clear and concise as possible. Assigning a symbol to a mathematical object may help us to do that, or it may do the opposite, or it may not make much difference either way (as is the case here). Often there are several different clear and concise ways to express a mathematical statement, and the one we use is just a matter of preference.

The next exercise asks you to try to recognise which statements from a list are correct alternative versions of a theorem from earlier in this unit. You may find it helpful to first identify the hypothesis and the conclusion of the theorem, but try also to recognise the correct versions simply by interpreting the language used in each statement in a natural way.

Exercise B148

Consider the following theorem from Subsection 2.1.

Theorem B75

Let G be a group of even order. Then G contains an element of order 2.

- (a) Which of the following are correct versions of this theorem?
 1. Every group of even order contains an element of order 2.
 2. Let G be a group that contains an element of order 2. Then G has even order.
 3. A group contains an element of order 2 provided that the group has even order.
 4. If G is a group of even order and $x \in G$, then x has order 2.
 5. If a group contains an element of order 2, then the group has even order.
 6. If G is a group of even order, then G contains an element of order 2.
- (b) Which of the correct versions of the theorem from part (a) do you think are good ways to state the theorem?
- (c) Which of statements 1–6 in part (a) state the converse of the theorem?
- (d) Is the converse true? Briefly justify your answer.

This subsection cannot of course describe all the many different ways in which theorems can be expressed. The theorem below, from Subsection 3.4 of Unit B2, has a format that is not the same as that of any of the theorems that you have seen so far in this subsection. It starts with a sentence of the form ‘Let ...’. As always, this sets up a condition that we are to assume holds for the remainder of the statement of the theorem. The theorem then asserts that a particular statement always holds under this condition. This statement is an implication.

The theorem is headed ‘Lemma’ rather than ‘Theorem’ because, as you saw in Unit A3, this word is used for theorems that are used in the proofs of other theorems.

Lemma B42

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. If m is a factor of n , then m has order n/m .

In the next exercise you are asked to rephrase this theorem as an implication.

Exercise B149

- (a) Rephrase Lemma B42 in the form 'If ..., then ...'. Hence state its hypothesis (or hypotheses) and conclusion (or conclusions).
- (b) Which of the following are correct versions of Lemma B42?
 1. If m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$, then m has order n/m provided that m is a factor of n .
 2. If m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$ and m has order n/m , then m is a factor of n .
 3. If the non-zero element m of the group $(\mathbb{Z}_n, +_n)$ is a factor of n , then it has order n/m .

The theorem below, from Subsection 3.2 of Unit B2, is expressed with a structure very like that of Lemma B42 above: it uses a sentence of the form 'Let ...' to set up a condition, then it asserts that a statement holds under this condition. However, here the statement is an *equivalence* rather than an implication.

Theorem B34

Let G be a finite group of order n . Then G is cyclic if and only if G contains an element of order n .

Remember from Unit A3 that an **equivalence** is a statement of the form ' P if and only if Q ', where P and Q are statements. It asserts that *both* of the implications 'If P then Q ' and 'If Q then P ' hold. It can also be expressed as ' $P \iff Q$ ', and in other ways too.

So Theorem B34 states that *both* of the following theorems hold.

Theorem B34 ('if' part)

Let G be a finite group of order n . If G contains an element of order n , then G is cyclic.

Theorem B34 ('only if' part)

Let G be a finite group of order n . If G is cyclic, then G contains an element of order n .

Exercise B150

- (a) Rephrase the 'if' part of Theorem B34 in the form 'If ..., then ...'. Hence state its hypothesis (or hypotheses) and conclusion (or conclusions).
- (b) Carry out part (a) for the 'only if' part.

Exercise B151

The following theorem is from Subsection 3.4 of Unit B2.

Corollary B40

Let $m \in \mathbb{Z}_n$. Then m is a generator of the group $(\mathbb{Z}_n, +_n)$ if and only if m is coprime to n .

- (a) State the 'if' and the 'only if' parts of this theorem, expressing both in the form 'If ..., then ...'.
- (b) State the hypothesis (or hypotheses) and conclusion (or conclusions) of the 'if' part.
- (c) Carry out part (b) for the 'only if' part.

Finally in this subsection, we will revisit one more useful idea about theorems that can be written in the form 'If P , then Q ', that is, $P \implies Q$. Remember from Unit A3 that the implication

$$P \implies Q$$

is equivalent to the implication

$$\text{not } Q \implies \text{not } P,$$

and that the second implication here is called the **contrapositive** of the first implication. Since an implication and its contrapositive are equivalent, saying that an implication is true is the same as saying that its contrapositive is true.

The contrapositive of a theorem provides a useful alternative interpretation of the theorem, which can be helpful when we want to apply the theorem. Also, sometimes the contrapositive of a theorem is simpler to prove than the original theorem.

Worked Exercise B50

Consider again the following theorem, from Subsection 3.2 of Unit B2. Write it in the form 'If ..., then ...', and hence write down its contrapositive.

Theorem B35

Every cyclic group is abelian.

Solution

The theorem can be written as:

If G is a cyclic group, then G is abelian.

 The theorem is of the form $P \implies Q$, where

P is: G is a cyclic group,

Q is: G is abelian,

not P is: G is not a cyclic group,

not Q is: G is not abelian. 

The contrapositive is:

If G is not abelian, then G is not a cyclic group.

 We can state this a little more clearly. 

It can also be stated as:

If a group is not abelian, then it is not cyclic.

Make sure that you do not confuse the *contrapositive* of an implication with the *converse* of an implication. Notice the difference between the contrapositive of the implication in Worked Exercise B50, and the converse of the same implication, which is

if G is an abelian group, then G is cyclic.

This converse is false, as you saw in Exercise B147.

Exercise B152

The following theorem is from Subsection 3.2 of Unit B2. Write it in the form 'If ..., then ...', and hence write down its contrapositive.

Theorem B36

Every subgroup of a cyclic group is cyclic.

3.2 Producing proofs

At first, being asked to produce a proof may feel like being asked to perform a magic trick. However, with the right support and preparation, and a good deal of practice, anyone can perform a magic trick! In the same way, learning to produce proofs requires support, preparation and practice.

There are usually two stages to producing a proof: *constructing* it, where you work out how to do it and sketch out a rough version, and *writing* it, where you explain it clearly in a form intended for someone else (or yourself at a later time) to read and understand.

Constructing a proof can be a bit like solving a puzzle: sometimes you may see immediately how to do it, but more often you will need to try out various ideas until one works. Often several different ideas will work, but some may work in a nicer – more elegant – way than others.

Usually a good approach to trying to construct a proof is to:

- write down *what you know*
- think about *what you want to prove*
- try to *bridge the gap* in an inspired way, using results and axioms that you already know.

Do not despair! Professional mathematicians regularly cover many pages with mathematics trying to find a way to prove something, and then cover even more trying to find a *nice* way to do it! Many people enjoy the challenge of doing this.

Once you think you have found a proof that works, and sketched out a rough version, you need to write it out clearly to explain it to others. You should aim to include enough explanation so that your reader does not have to rethink too much of the argument, but not so much explanation that the main argument is obscured. You should follow the usual principles of good mathematical writing: for example, you should write in sentences, use notation correctly and introduce all variables before using them. A finished proof produced by a professional mathematician, such as those given in this module, will usually have been significantly rewritten and ‘polished’ from the version that was first written down. Writing good proofs can be an art, one that develops with practice and reveals a little of the writer’s individual style.

Sometimes, if a proof is straightforward, you may find that you can do both the constructing and the writing at the same time. Also, when you produce a proof in an examination you will not have time to polish it much, so although the logic of your proof must be correct for full marks, a lower standard of proof writing (but not a poor standard) is acceptable.

As you will have noticed, the language used in proofs is sometimes slightly different from everyday English. For example, words such as *thus*, *hence*, *therefore*, *so* and *consequently* are useful for indicating which statements follow from which. Usually you can use these words interchangeably: you may prefer to avoid repeating the same word, or you may choose a consistent wording.

The one thing that holds for all proofs is that the logical reasoning must be sound: the proof must completely justify the statement that it is proving.



Paul Erdős

Proofs from 'the Book'

The idea that mathematicians constantly strive to produce perfect proofs was evocatively captured by the prolific Hungarian mathematician Paul Erdős (1913–1996) who famously conceived of a 'transfinite Book' in which God keeps the most perfect and elegant proof of each mathematical theorem. He used the word 'transfinite' to describe the Book because, as he said, it is 'a concept in mathematics that is larger than infinite'. It has been often recounted that when Erdős was lecturing at an American summer camp to a group of highly talented students, he told them: 'You don't have to believe in God, but you should believe in the Book.'

(Source: Hoffman, P. (1998) *The Man Who Loved Only Numbers*, Hyperion, p. 26)

The next two subsections are intended to help you build up your skills with proofs by practising reading and producing proofs in group theory. You will start with some simple proofs and build up to some that are a little harder.

Throughout these subsections we will use the concise multiplicative notation for abstract groups that was introduced in Subsection 2.1. That is, we will denote a composite of two elements x and y of a general group simply by xy rather than $x \circ y$.

3.3 Proofs using the group axioms

In this subsection we will start gently by looking at how some basic properties of group elements can be deduced directly from the group axioms and from simple properties of groups that you met earlier.

Most of the results here will not be new to you; our interest here is in how they can be proved. The idea is not for you to look up and emulate the proofs of these or similar results in earlier units, but to try to prove these results afresh, find inspiration and build up your confidence in constructing proofs. The methods of proof needed are all very similar.

Here is a reminder of the group axioms, which you met in Unit B1. They are stated here using the concise multiplicative notation mentioned above.

Definition

Let G be a set on which a binary operation is defined. Then G is a **group** if the following four axioms hold.

G1 Closure For all g, h in G ,

$$gh \in G.$$

G2 Associativity For all g, h, k in G ,

$$g(hk) = (gh)k.$$

G3 Identity There is an element e in G such that

$$ge = g = eg \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element**.)

G4 Inverses For each element g in G , there is an element h in G such that

$$gh = e = hg.$$

(The element h is an **inverse element** of g .)

As well as using the group axioms in our proofs, we will use the first two basic properties of groups that you met in Unit B1. These are restated below; they can be proved using the group axioms, as you saw earlier, and you may assume them throughout the rest of this section.

Propositions B11 and B12

In any group,

- the identity element is unique, and we denote it by e ,
- each element x has a unique inverse, which we denote by x^{-1} .



The next worked exercise demonstrates how a simple result can be proved using these properties and the group axioms.

Worked Exercise B51

Let G be a group and let x be an element of G .



Assuming only the group axioms and Propositions B11 and B12, prove that if g is an element of G such that $gx = x$, then $g = e$.

Solution

 Start by writing down what we are given – the hypothesis or hypotheses. When writing out our proof, we do not need to repeat the ‘Let ...’ sentence in the question, even though it contains hypotheses, because any sentence of this form in a theorem or question is assumed to apply throughout the proof. (However, it is often helpful to note down such hypotheses when trying to *construct* a proof.) 

Suppose that g is an element of G such that

$$gx = x.$$

 We want to get to $g = e$. Both sides of the given equation end in an x , so we try composing both sides with the inverse of x . 

Composing both sides of the equation on the right with the inverse of x gives

$$(gx)x^{-1} = xx^{-1}.$$

Hence

$$g(xx^{-1}) = xx^{-1} \quad (\text{by axiom G2, associativity}),$$

so

$$ge = e \quad (\text{by axiom G4, inverses}),$$

giving

$$g = e \quad (\text{by axiom G3, identity}),$$

as required.

You should usually finish a proof with some concluding words that confirm that the required result has been proved. For the simple proof in Worked Exercise B51, the final ‘as required’ serves this purpose.

The results in the following exercises can be proved using a method similar to that in Worked Exercise B51.

Exercise B153

Let G be a group and let a be an element of G .

Assuming only the group axioms and Propositions B11 and B12, prove that if $a^2 = a$ then $a = e$.

Exercise B154

Let G be a group, and let g and h be elements of G .

Assuming only the group axioms and Propositions B11 and B12, prove that if $gh = e$ then $h = g^{-1}$.

Note that the result in Exercise B154 is clearly true when the group G is abelian, because in that case the equation $gh = e$ is equivalent to the equation $hg = e$, giving $gh = e = hg$, which, by the definition of an inverse, implies that $h = g^{-1}$. The proof in the solution to Exercise B154 shows that the result also holds for non-abelian groups.

A more efficient way to prove the results in Worked Exercise B51 and Exercises B153 and B154 is to use the Cancellation Laws, which, as you saw in Unit B1, can be deduced from the group axioms. They are stated below, using concise multiplicative notation.

Proposition B15 Cancellation Laws

In any group G with elements a , b and x :

- if $xa = xb$, then $a = b$ (**Left Cancellation Law**)
- if $ax = bx$, then $a = b$ (**Right Cancellation Law**).

In the next worked exercise, the result in Worked Exercise B51 is proved using one of these laws. When you are trying to construct a proof, you should always consider whether you can apply results proved earlier.

Worked Exercise B52

Let G be a group and let x be an element of G .



Use one of the Cancellation Laws to prove that if g is an element of G such that $gx = x$, then $g = e$.

Solution

 As usual, we start by writing down what we are given. 

Let g be an element of G such that

$$gx = x.$$

 We want to get to $g = e$. Both sides of the given equation end in an x , so we use the Right Cancellation Law. 

By axiom G3 (identity), this equation can be written as

$$gx = ex,$$

so, by the Right Cancellation Law,

$$g = e,$$

as required.

The next two exercises ask you to repeat Exercises B153 and B154, this time using the Cancellation Laws.

Exercise B155

Let G be a group and let a be an element of G .

Use one of the Cancellation Laws to prove that if $a^2 = a$, then $a = e$.

Exercise B156

Let G be a group, and let g and h be elements of G .

Use one of the Cancellation Laws to prove that if $gh = e$, then $h = g^{-1}$.

As mentioned in Unit B1, as your familiarity with group theory grows you can start to merge some of the steps in your proofs, and not mention the group axioms every time you use them. You just need to make sure that the reasoning behind each step of your proof is either explained or will be immediately clear to a reader whose familiarity with group theory is about the same as yours. The proofs in the module texts will give you an idea of how much detail is required.

Also, you do not need to use brackets in composites of three or more group elements, since, as discussed in Unit B1, axiom G2 (associativity) tells us that the positioning of these brackets does not affect the overall composite, as long as the order of the group elements in the composite remains unchanged.

For example, here is a shorter version of the proof in Worked Exercise B51. The method is exactly the same.

Worked Exercise B53

Let G be a group and let x be an element of G .

Prove that if g is an element of G such that $gx = x$, then $g = e$.

Solution

Let $g \in G$ be such that

$$gx = x.$$

Composing both sides on the right with x^{-1} gives

$$gxx^{-1} = xx^{-1},$$

so

$$ge = e,$$

giving

$$g = e,$$

as required.

Even though brackets are not needed in composites of group elements, sometimes it can be helpful to include them, as they can make the reasoning clearer.

The results in the next two exercises can be proved using ideas similar to those that have been used in this subsection so far. You have seen Exercise B157 before, in Unit B1, but do not look back there: try it anew.

Exercise B157

Let G be a group and let a , b and c be elements of G .

Prove that if $abc = e$, then $bca = e$.

The exercise below involves the idea of two group elements *commuting*. We say that elements x and y of a group G **commute** if $xy = yx$. Thus all pairs of elements in an abelian group commute, but only some do in a non-abelian group.

Exercise B158

Let G be a group and let x and y be elements of G .

Prove that if x and y commute, then $y = xyx^{-1}$.

In the next exercise you have to try to think of a method for proving the proposition below, which is from Unit B1 and is stated here using concise multiplicative notation. You will need to think about the definition of the inverse of a group element. There is more than one way to prove this result. Do not look back at the proof provided in Unit B1!

Proposition B14

Let x and y be elements of a group G . Then

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Exercise B159

Let G be a group, and let x and y be elements of G .

Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

It is important to remember Proposition B14, as it comes up frequently when we are working with group elements.

In the next exercise you will need to think about what the terms *self-inverse* and *abelian* mean, and work out a way to get from one to the other. There are different ways to do this: for example, one method involves using the group axioms, and another involves using Proposition B14.

Exercise B160

Let G be a group in which every element is self-inverse.

Prove that G is abelian.

In fact, the result in Exercise B160 is equivalent to Theorem B73 in Subsection 2.1, so you have essentially already seen a proof of it.

We end this subsection with a proof that is a little different from those in this section so far, and possibly a little tougher. It involves using *proof by induction*, which you met in Unit A3. It provides part of the proof of a result that you met in Unit B2, namely Theorem B27(c).

Remember that when you want to prove by induction that a statement $P(n)$ holds for all natural numbers n , you should proceed as follows.

1. Identify the statement $P(n)$, and state it clearly.
2. Show that $P(1)$ holds.
3. Assume that $P(k)$ holds for a general natural number k , and write down $P(k)$.
4. State that we need to deduce $P(k + 1)$, and write down $P(k + 1)$.
5. Deduce $P(k + 1)$ from $P(k)$.
6. Conclude that $P(n)$ holds for all natural numbers n .

Exercise B161

Let G be a group and let x be an element of G .

Use mathematical induction to prove that $(x^n)^{-1} = (x^{-1})^n$ for all $n \in \mathbb{N}$.

3.4 Proofs involving subgroups

In this subsection we will look at some results about subgroups. This will provide you with further practice in reading and writing proofs. You will also meet a few results that have not appeared earlier in this book.

Here is a reminder of the definition of a subgroup, from Subsection 1.1 of Unit B2.

Definition

A **subgroup** of a group (G, \circ) is a group (H, \circ) , where H is a subset of G .

The definition includes the symbol \circ for the binary operation of the group G ; it is retained here to make it clear that a subgroup of a group must have the same binary operation as the group. In this subsection, while keeping this condition in mind, we will continue to use concise multiplicative notation for abstract groups – that is, we will not use a symbol for the binary operation.

Some of the proofs in this subsection involve showing that a particular subset of a group is, or is not, a subgroup. In Unit B2 you saw that you can do this by considering three properties, called the **subgroup properties**, as stated in the following theorem.

Theorem B24 Subgroup test

Let G be a group and let H be a subset of G . Then H is a subgroup of G if and only if the following three properties hold.

SG1 Closure For all x, y in H , the composite xy is in H .

SG2 Identity The identity element e of G is in H .

SG3 Inverses For each x in H , its inverse x^{-1} is in H .

We start by proving the useful result that the intersection of any two subgroups is also a subgroup.

Worked Exercise B54

Let H and K be subgroups of a group G .

Prove that the set $H \cap K$ is a subgroup of G .

Solution

We check the three subgroup properties.

SG1 Let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$.

 Use the fact that H and K are subgroups. 

Since $x, y \in H$ and H is a subgroup of G , we have $xy \in H$.
Likewise $xy \in K$. Hence $xy \in H \cap K$. Thus $H \cap K$ is closed.

SG2 Since H and K are subgroups of G , we have $e \in H$ and $e \in K$.
Hence $e \in H \cap K$.

SG3 Let $x \in H \cap K$. Then $x \in H$ and $x \in K$.

Since $x \in H$ and H is a subgroup of G , we have $x^{-1} \in H$.
Likewise $x^{-1} \in K$.

Hence $x^{-1} \in H \cap K$. Thus $H \cap K$ contains the inverse of each of its elements.

Hence $H \cap K$ satisfies the three subgroup properties, so it is a subgroup of G .

The subgroups H and K in Worked Exercise B54 are interchangeable, so when we had to prove a fact about K that we had already proved for H , we did not give the full details but instead used the word *likewise*. This

removed unnecessary detail from the proof, making it less cluttered and therefore quicker and easier to follow. Other words and phrases that can be used in place of *likewise* include *similarly* and *in a similar way*.

It is worth stating the result proved in Worked Exercise B54 as a theorem, so we can conveniently refer to it later.

Theorem B81

Let H and K be subgroups of a group G . Then $H \cap K$ is also a subgroup of G .

In the next exercise, rather than immediately launching into a proof similar to that in Worked Exercise B54, think carefully about what you know already that might be helpful.

Exercise B162

Let G be a group with subgroups H and K .

Prove that the set $H \cap K$ is a subgroup of H .

We can now say that, similarly, if H and K are subgroups of a group G , then $H \cap K$ is a subgroup of K .

We now know that intersections of subgroups are subgroups, but what about unions of subgroups?

Worked Exercise B55


Show that the following statement is false.

If H and K are subgroups of a group G , then the set $H \cup K$ is a subgroup of G .

Solution

 Remember that the statement really means the following.

For all groups G and subgroups H and K of G , the set $H \cup K$ is a subgroup of G .

It is a *universal statement*. So to show that it is not true, we find a counterexample. We can try taking G to be a small, familiar group, and H and K to be subgroups that are easy to find, such as cyclic subgroups. 

Let



$$G = S(\square) = \{e, a, r, s\},$$

$$H = \langle a \rangle = \{e, a\},$$

$$K = \langle r \rangle = \{e, r\}.$$



Then

$$H \cup K = \{e, a, r\}.$$

 We need to show that this is not a subgroup. We can do this by showing that *any one* of the three subgroup properties fails. Here we can show that property SG1 (closure) fails. 

Now $a, r \in H \cup K$, and

$$a \circ r = s.$$

 A quick way to work out that $a \circ r = s$ is to use the fact that $S(\square)$ is isomorphic to the Klein four-group V , in which the composite of any two distinct non-identity elements is the third non-identity element (as mentioned at the end of Subsection 2.3). 

However, $s \notin H \cup K$, so $H \cup K$ is not closed; that is, property SG1 fails. Hence $H \cup K$ is not a subgroup of G .

This counterexample shows that the given statement is false.

In Worked Exercise B55 we chose the group $S(\square)$ as a counterexample, but most of the other small groups that you have met would have worked just as well. Once we had chosen two subgroups of $S(\square)$, we showed that their union is not a subgroup by showing that it is not closed, but we could instead have used Lagrange's Theorem, as follows. The set $H \cup K = \{e, a, s\}$ has order 3, so by Lagrange's Theorem it cannot be a subgroup of $S(\square)$, since 3 does not divide 4.

Exercise B163

Show that the following statement is false.

If H and K are subgroups of a group G , then the set $H \cup K$ is never a subgroup of G .

Worked Exercise B55 and Exercise B163 together show that if H and K are subgroups of a group G , then the subset $H \cup K$ may or may not be a subgroup of G .

The solution to Exercise B163 illustrates that when you are trying to find a counterexample it is often helpful to start by looking for very simple possibilities. In the next exercise finding a counterexample is not quite so straightforward.

Exercise B164

Show that the following statement is false.

If H and K are distinct non-trivial proper subgroups of a group G , then the set $H \cup K$ is never a subgroup of G .

The next exercise asks you to prove a theorem from Unit B2. As before, try this without looking back to where the proof was first given.

Exercise B165

Prove the theorem below, using the definition that if x is an element of a group G , then $\langle x \rangle$ is the subset of G given by

$$\langle x \rangle = \{x^k : k \in \mathbb{Z}\}.$$

Theorem B32

Let x be an element of a group G . Then $\langle x \rangle$ is a subgroup of G .

Here are some more exercises involving subgroups for you to try. The result in Exercise B167 is justified in Subsection 1.1 of Unit B2, but, as usual, do not look back. Exercises B168 and B169 require more thought than Exercises B166 and B167.

Exercise B166

Let H be a subgroup of a group G , and let K be a subgroup of H . Prove that K is a subgroup of G .

Exercise B167

Prove that every subgroup of an abelian group is abelian.

Exercise B168

Let G be a group and let H and K be *distinct* subgroups of G of the same prime order.

Using Theorem B81 and Lagrange's Theorem, prove that $H \cap K = \{e\}$.

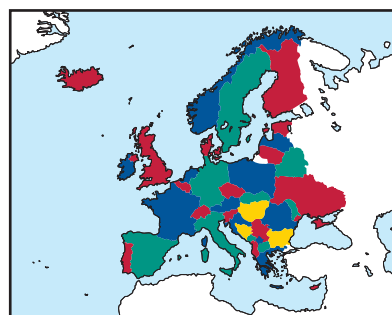
Exercise B169

Let G be a group and let H and K be subgroups of G of coprime orders.

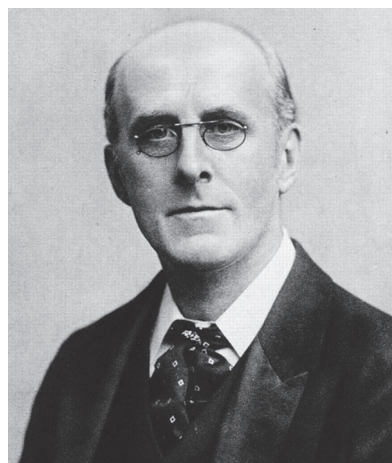
Using Theorem B81 and Lagrange's Theorem, prove that $H \cap K = \{e\}$.

3.5 Checking proofs

It is easy to make errors in proofs, so an important skill in mathematics is carefully reading mathematical arguments and spotting any problems. This is important not only for checking your own proofs, but also for checking those proposed by other people. Many people, when they do this kind of checking, tend to concentrate on the 'visible' mathematical working, such as algebraic manipulations. However, errors often lie elsewhere. For example, a logical deduction may be invalid, a definition or a theorem may have been misinterpreted, something may have been assumed that is not necessarily true, or there may be cases that have not been considered. It is important to try to look out for these sorts of problems.



A map of Europe coloured with four colours



Alfred Bray Kempe

Famous errors in proofs

In 1871, the London barrister and keen mathematician Alfred Bray Kempe (1849–1922) published a 'proof' of the so-called *four-colour problem*. This problem, which asks whether every map can be coloured with at most four colours in such a way that neighbouring countries are coloured differently, had first been posed in 1852. Kempe's proof, which appeared in the newly founded *American Journal of Mathematics*, aroused considerable interest and was widely accepted. It was a very good proof – it was incorrect, but it was a very good incorrect proof! It contained sound ideas and it convinced mathematicians for 11 years until an error was found by another British mathematician, Percy John Heawood (1861–1955). The flaw in Kempe's argument turned out to be serious and, despite extensive efforts of mathematicians in Europe and in the United States, it was not until 1976 that Kenneth Appel (1932–2013) and Wolfgang Haken (1928–) found a correct proof. Their famous proof, which was several hundred pages long, had required 1000 hours of computer time. This in turn sparked a new debate: can a proof be accepted as valid if it cannot be checked by hand?

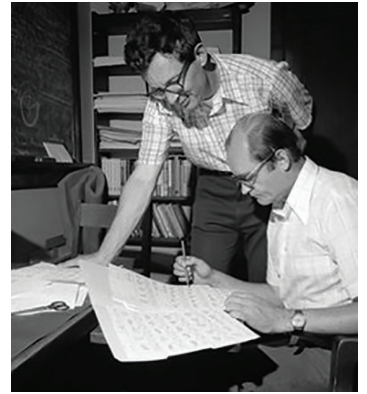
Other notable errors include one by the great French mathematician Henri Poincaré (1854–1912), who realised that he had made a crucial mistake in his original prize-winning paper of 1889 on the three-body problem. But his realisation came only after the paper had been printed and copies distributed, though fortunately before the journal in which it was due to appear had been published. Nevertheless, Poincaré had to pay for the reprinting, which cost him more than the prize he had won! Famously, it was in correcting the mistake that he discovered the foundations of what today is known as *mathematical chaos*.

A more recent example is that of Andrew Wiles' (1953–) celebrated proof of Fermat's Last Theorem. The theorem had withstood attack for over 350 years when in 1993 Wiles, after seven years of work, first presented his proof, generating a great amount of excitement. Wiles' manuscript was sent for review prior to publication and it was only then that Wiles realised there was a critical hole in his proof. A year passed and Wiles was about to give up trying to repair it when he suddenly saw how it could be done. Together with his former student Richard Taylor (1962–), Wiles repaired the hole and the 129-page proof was finally published in 1995.

To check a proof, you need to read it through, very carefully, from start to finish, making sure that the correct assumptions have been used (such as the correct hypotheses), and that at each step of the argument you are convinced that each new statement does indeed follow logically from previous statements (and from other known facts). You might find it helpful to try explaining each step to yourself in different words. When you reach the end you should make sure that the correct conclusions have been reached. And you do need to check any algebraic manipulations!

If a proof uses a particular method of proof, such as proof by contradiction, proof by contraposition or proof by induction, then you need to make sure that the method has been applied correctly. In particular, for a proof by contradiction you should check that the correct negation has been used, and for a proof by contraposition you should check that the correct contrapositive has been used.

The worked exercise below contains two 'attempted proofs' of a theorem from earlier in this unit and asks whether the attempts are correct. Before you look at the solution, you might like to try checking the attempted proofs for yourself.



Kenneth Appel (left) and Wolfgang Haken



Henri Poincaré



Andrew Wiles

Worked Exercise B56

Consider the following theorem from Subsection 2.1 of this unit.

Theorem B75

Let G be a group of even order. Then G contains an element of order 2.

Determine whether the following two attempted proofs of this theorem are correct. For each one that is incorrect, explain why.

Proof attempts (may be incorrect!)**Attempt 1**

The group G has even order, so 2 divides the order of G . By Lagrange's Theorem, G has a subgroup of order 2, and such a subgroup is generated by an element of order 2. Thus G has an element of order 2.

Attempt 2

We prove the contrapositive. Let G be a group of odd order, and let g be any element of G . By Lagrange's Theorem, the order of the subgroup $\langle g \rangle$ must divide the order of G , so the order of $\langle g \rangle$ cannot be 2. Therefore g does not have order 2. Thus G does not have any elements of order 2. Since the contrapositive is true, the original statement is also true.

Solution**Attempt 1**

This attempted proof is incorrect. The problem occurs in the step 'By Lagrange's Theorem, G has a subgroup of order 2'. Lagrange's Theorem tells us that the only possible orders for a subgroup of a group are the positive divisors of the order of the group, but it does not say that there *is* a subgroup of each of these possible orders.

Attempt 2

This attempted proof is also incorrect. It provides a correct proof of the following statement:

If G is a group of odd order, then G has no element of order 2.

However, this statement is not the contrapositive of the result that is to be proved, nor is it equivalent to the result to be proved for any other reason. The correct contrapositive is as follows.

If G is a group with no element of order 2, then G has odd order.

In fact the statement proved in Attempt 2 in Worked Exercise B56 is equivalent to the *converse* of Theorem B75.

Exercise B170

Below are four further attempted proofs of Theorem B75, the theorem stated in Worked Exercise B56.

Determine which, if any, of these attempted proofs are correct. For each one that is incorrect, explain why.

Proof attempts (may be incorrect!)

Attempt 3

The group $S(\square)$ has even order (it has order 4), and every non-identity element in $S(\square)$ has order 2. Thus a group of even order has an element of order 2.

Attempt 4

Let G be a group with an element of order 2, say g . Then $\langle g \rangle = \{e, g\}$ is a subgroup of G of order 2. By Lagrange's Theorem, since G has a subgroup of order 2, the order of G must be divisible by 2, that is, it must be even. This proves the result.

Attempt 5

Let G be a group with no element of order 2. Then every non-identity element g in G has an inverse g^{-1} that is not equal to g . These elements g and g^{-1} are inverses of each other, so every element of G , except the identity, comes in a pair. Therefore G has an odd number of elements, and so has odd order. Thus the contrapositive of the original statement is true and therefore the original statement is also true.

Attempt 6

Let G be a group of even order. We use proof by contradiction. Suppose that G does not contain an element of order 2. Then there is no element x of G that satisfies the equation $x^2 = e$. This equation is equivalent to the equation $x = x^{-1}$. However, there is an element of G that satisfies this equation, namely the identity element e , since $e = e^{-1}$. This contradiction shows that the assumption that G does not contain an element of order 2 is incorrect. Hence G does contain an element of order 2, which proves the required result.

In the final exercise in this unit you are asked to find an error in a proof and fix it.

Exercise B171

Consider the following (true) statement and attempted proof.

Statement

Let G be a finite group. Then the orders of ab and ba are the same for every a, b in G .

Proof attempt (incorrect!)

Let $a, b \in G$. Since G is finite, both ab and ba have finite order. Suppose that ab has order n . Then

$$(ab)^n = e,$$

that is,

$$\underbrace{abab \cdots ab}_{n \text{ copies of } ab} = e.$$

Composing both sides on the left with a^{-1} and on the right with a gives

$$a^{-1}a \underbrace{baba \cdots ba}_{n-1 \text{ copies of } ba} ba = a^{-1}ea,$$

that is,

$$\underbrace{baba \cdots ba}_{n \text{ copies of } ba} = e,$$

which we can write as

$$(ba)^n = e.$$

Hence ba also has order n .

Thus the orders of ab and ba are the same. This completes the proof.

- (a) Contrary to the final sentence, the proof is incomplete. Explain what the problem is.

Hint: Think carefully about the definition of the order of a group element.

- (b) Provide the missing portion of the proof.

Summary

In this unit you have met Lagrange's Theorem, one of the most fundamental theorems in group theory. You have seen how by using this theorem together with other theorems from earlier in this book we can determine the different isomorphism classes for groups of orders 1 to 7, and you have met the isomorphism classes for groups of order 8. You have also practised working with theorems and proofs, which are crucial components of pure mathematics. Now that you have reached this point, you should be starting to appreciate the beauty of group theory, and the power of the type of abstract approach that it exemplifies. You should be ready to go on to the deeper group theory presented in Book E.

Learning outcomes

After studying this unit, you should be able to:

- understand and apply Lagrange's Theorem and its corollaries
- understand the structure of all groups of prime order
- describe the isomorphism classes for groups of orders 1 to 8
- determine the isomorphism class to which a given group of order 8 or less belongs
- understand and apply theorems expressed in a variety of different ways
- read and understand simple proofs in group theory
- prove simple results in group theory
- check simple proofs.

Solutions to exercises

Solution to Exercise B131

It follows from Lagrange’s Theorem (Theorem B68) that in each case the possible orders of the subgroups are the positive divisors of n .

- (a) The possible orders are 1, 2, 4, 5, 10 and 20.
- (b) The possible orders are 1, 5 and 25.
- (c) The possible orders are 1 and 29.

Solution to Exercise B132

In each case there are several possibilities for the array, depending on which element we choose each time there is a choice to be made. If we always choose the first possible element from the list e, a, b, c, r, s, t, u , then we obtain the following arrays.

- (a)

e

b

a

c

r

t

s

u
- (b)

e

a

b

c

r

u

t

s

Solution to Exercise B133

The table below contains a complete list of all the subgroups of A_4 together with their orders.

Order	Subgroup of A_4
1	$\{e\}$
2	$\{e, (1\ 2)(3\ 4)\}$
2	$\{e, (1\ 3)(2\ 4)\}$
2	$\{e, (1\ 4)(2\ 3)\}$
3	$\langle (1\ 2\ 3) \rangle = \langle (1\ 3\ 2) \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$
3	$\langle (1\ 2\ 4) \rangle = \langle (1\ 4\ 2) \rangle = \{e, (1\ 2\ 4), (1\ 4\ 2)\}$
3	$\langle (1\ 3\ 4) \rangle = \langle (1\ 4\ 3) \rangle = \{e, (1\ 3\ 4), (1\ 4\ 3)\}$
3	$\langle (2\ 3\ 4) \rangle = \langle (2\ 4\ 3) \rangle = \{e, (2\ 3\ 4), (2\ 4\ 3)\}$
4	$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
12	A_4

All the subgroups of A_4 , except the one of order 4 and A_4 itself, are cyclic subgroups. The subgroup of order 4 represents the symmetry group of the labelled rectangle below.



Solution to Exercise B134

- (a) The order of S_4 is $4! = 24$.
The permutation $(1\ 2\ 3\ 4)$ is a 4-cycle and so has order 4.
Hence the order of $(1\ 2\ 3\ 4)$ divides the order of S_4 .
- (b) As in part (a), the order of S_4 is $4! = 24$.
The permutation $(1\ 3\ 4)$ is a 3-cycle and so has order 3.
Hence the order of $(1\ 3\ 4)$ divides the order of S_4 .
- (c) The order of $(\mathbb{Z}_9, +_9)$ is 9.
The consecutive multiples of 5 in $(\mathbb{Z}_9, +_9)$ are

$\dots, 0, 5, 1, 6, 2, 7, 3, 8, 4, 0, \dots,$

so the order of 5 in $(\mathbb{Z}_9, +)$ is 9.
Hence the order of 5 divides the order of $(\mathbb{Z}_9, +_9)$.
- (d) As in part (c), the order of $(\mathbb{Z}_9, +_9)$ is 9.
The consecutive multiples of 6 in $(\mathbb{Z}_9, +_9)$ are

$\dots, 0, 6, 3, 0, \dots,$

so the order of 6 in $(\mathbb{Z}_9, +)$ is 3.
Hence the order of 6 divides the order of $(\mathbb{Z}_9, +_9)$.

Solution to Exercise B135

- (a) The group G has order 5, which is a prime number, so G is cyclic, by Corollary B70.
- (b) The identity element in the group is y , because the row and column labelled y repeat the borders of the table.

To verify that the other elements have order 5, we calculate their successive powers, using the information in the Cayley table. We have

$$\begin{aligned}v^2 &= v \circ v = w, \\v^3 &= v^2 \circ v = w \circ v = z, \\v^4 &= v^3 \circ v = z \circ v = x, \\v^5 &= v^4 \circ v = x \circ v = y,\end{aligned}$$

so v has order 5. Similarly,

$$\begin{aligned}w^2 &= w \circ w = x, \\w^3 &= w^2 \circ w = x \circ w = v, \\w^4 &= w^3 \circ w = v \circ w = z, \\w^5 &= w^4 \circ w = z \circ w = y,\end{aligned}$$

so w has order 5;

$$\begin{aligned}x^2 &= x \circ x = z, \\x^3 &= x^2 \circ x = z \circ x = w, \\x^4 &= x^3 \circ x = w \circ x = v, \\x^5 &= x^4 \circ x = v \circ x = y,\end{aligned}$$

so x has order 5;

$$\begin{aligned}z^2 &= z \circ z = v, \\z^3 &= z^2 \circ z = v \circ z = x, \\z^4 &= z^3 \circ z = x \circ z = w, \\z^5 &= z^4 \circ z = w \circ z = y,\end{aligned}$$

so z has order 5.

(c) The group G has generators w, x, v and z .

The group $(\mathbb{Z}_5, +_5)$ has generators 1, 2, 3 and 4.

Using the technique of matching powers of the generators w and 1, we obtain the following isomorphism.

$$\begin{aligned}\phi : G &\longrightarrow \mathbb{Z}_5 \\y &\longmapsto 0 \\w &\longmapsto 1 \\w \circ w &\longmapsto 1 +_5 1 \\w \circ w \circ w &\longmapsto 1 +_5 1 +_5 1 \\w \circ w \circ w \circ w &\longmapsto 1 +_5 1 +_5 1 +_5 1\end{aligned}$$

This simplifies to the following.

$$\begin{aligned}\phi : G &\longrightarrow \mathbb{Z}_5 \\y &\longmapsto 0 \\w &\longmapsto 1 \\x &\longmapsto 2 \\v &\longmapsto 3 \\z &\longmapsto 4\end{aligned}$$

(There are three other isomorphisms, obtained from $w \mapsto 2$, $w \mapsto 3$ and $w \mapsto 4$.)

Solution to Exercise B136

(a) Since $|G| = 14$, the possible orders of proper subgroups of G are 1, 2 and 7, by Lagrange's Theorem.

The trivial subgroup has order 1, so is certainly cyclic. Also, since 2 and 7 are primes, any subgroup of G of order 2 or 7 is cyclic, by Corollary B70 to Lagrange's Theorem.

Thus every proper subgroup of G is cyclic.

(b) We generalise the argument in part (a). Since $|G| = pq$, where both p and q are primes, the possible orders of proper subgroups of G are 1, p and q , by Lagrange's Theorem.

The trivial subgroup has order 1, so is certainly cyclic. Also, since p and q are primes, any subgroup of G of order p or q is cyclic, by Corollary B70 to Lagrange's Theorem.

Thus every proper subgroup of G is cyclic.

Solution to Exercise B137

(a) (i) The statement $ex = x$ is rewritten as $e \circ x = x$.

(ii) The statement $x^2x^3 = x^5$ is rewritten as $x^2 \circ x^3 = x^5$.

(iii) The statement $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$ is rewritten as

$$(x \circ y \circ z)^{-1} = z^{-1} \circ y^{-1} \circ x^{-1}.$$

(iv) The statement $x^0 = e$ does not need to be rewritten.

(v) The statement $xy = xz \implies y = z$ is rewritten as

$$x \circ y = x \circ z \implies y = z.$$

(b) (i) The statement $ex = x$ is rewritten as

$$0 + x = x.$$

(ii) The statement $x^2x^3 = x^5$ is rewritten as

$$2x + 3x = 5x.$$

(iii) The statement $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$ is rewritten as

$$-(x + y + z) = (-z) + (-y) + (-x),$$

or, since every additive group is abelian,

$$-(x + y + z) = (-x) + (-y) + (-z).$$

(iv) The statement $x^0 = e$ is rewritten as

$$0x = 0.$$

(v) The statement $xy = xz \implies y = z$ is rewritten as

$$x + y = x + z \implies y = z.$$

Solution to Exercise B138

Let G be a group in which each element except the identity has order 2, and let x and y be elements of G . We have to show that $xy = yx$. Since $xy \in G$ and since $g = g^{-1}$ for each $g \in G$, we have

$$\begin{aligned} xy &= (xy)^{-1} \\ &= y^{-1}x^{-1} \\ &= yx. \end{aligned}$$

Thus G is abelian.

Solution to Exercise B139

(a) The orders of the elements are as follows.

Element	e	$(1\ 3)$	$(2\ 5)$	$(1\ 3)(2\ 5)$
Order	1	2	2	2

Since the group contains no element of order 4, it is isomorphic to V .

(b) The orders of the elements are as follows.

Element	e	$(2\ 3\ 4\ 6)$	$(2\ 4)(3\ 6)$	$(2\ 6\ 4\ 3)$
Order	1	4	2	4

Since the group contains an element of order 4, it is isomorphic to C_4 .

(The group in part (b) is the cyclic subgroup generated by $(2\ 3\ 4\ 6)$ or by $(2\ 6\ 4\ 3)$.)

Solution to Exercise B140

There are many possible answers.

(a) Any cyclic subgroup of S_6 of order 6 is isomorphic to C_6 . One possibility is the subgroup generated by the permutation $(1\ 2\ 3\ 4\ 5\ 6)$:

$$\begin{aligned} &\langle (1\ 2\ 3\ 4\ 5\ 6) \rangle \\ &= \{e, (1\ 2\ 3\ 4\ 5\ 6), (1\ 3\ 5)(2\ 4\ 6), \\ &\quad (1\ 4)(2\ 5)(3\ 6), (1\ 5\ 3)(2\ 6\ 4), (1\ 6\ 5\ 4\ 3\ 2)\}. \end{aligned}$$

(b) Any non-abelian subgroup of S_6 of order 6 is isomorphic to $S(\triangle)$. One possibility is the subgroup

$$\{e, (2\ 3), (2\ 6), (3\ 6), (2\ 3\ 6), (2\ 6\ 3)\}$$

obtained by labelling the vertices of the equilateral triangle with the symbols 2, 3 and 6.

Solution to Exercise B141

We know that (U_{15}, \times_{15}) is a group, by Theorem B9 in Unit B1. It is abelian, since \times_{15} is a commutative binary operation.

We have

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\},$$

so (U_{15}, \times_{15}) has order 8.

The identity element 1 has order 1.

The consecutive powers of 2 in (U_{15}, \times_{15}) are

$$\dots, 1, 2, 4, 8, 1, 2, 4, 8, \dots,$$

so 2 has order 4. The element immediately before the identity element 1 in the cycle of powers of 2 is 8, so 8 is the inverse of 2 and hence it also has order 4. Also, the cycle above shows that the consecutive powers of $4 = 2^2$ are

$$\dots, 1, 4, 1, 4, 1, 4, \dots,$$

so 4 has order 2.

The consecutive powers of 7 are

$$\dots, 1, 7, 4, 13, 1, 7, 4, 13, \dots,$$

So 7 has order 4, and 13, the inverse of 7, also has order 4.

The consecutive powers of 11 are

$$\dots, 1, 11, 1, 11, \dots$$

So 11 has order 2.

The consecutive powers of 14 are

$$\dots, 1, 14, 1, 14, \dots$$

So 14 has order 2.

In summary, the orders of the elements of (U_{15}, \times_{15}) are as follows.

Element	1	2	4	7	8	11	13	14
Order	1	4	2	4	4	2	4	2

So (U_{15}, \times_{15}) is an abelian group of order 8 that has four elements of order 4 and three elements of order 2.

(When you are carrying out calculations in modular arithmetic like those above, remember that there are ways to make your calculations quicker and easier, as you saw in Unit A2 *Number systems*. For example, to work out 14^2 in (U_{15}, \times_{15}) , instead of starting by working out $14^2 = 196$, you can proceed as follows:

$$14^2 \equiv 14 \times 14 \equiv (-1) \times (-1) \equiv 1 \pmod{15}.$$

Thus $14 \times_{15} 14 = 1$.)

Solution to Exercise B142

The Cayley table for Q_8 shows that the identity element of Q_8 is 1. Also, by the Cayley table, we have

$$i^2 = -1,$$

$$i^3 = i^2 i = (-1)i = -i,$$

$$i^4 = i^3 i = (-i)i = 1,$$

and

$$(-i)^2 = -1,$$

$$(-i)^3 = (-i)^2(-i) = (-1)(-i) = i,$$

$$(-i)^4 = (-i)^3(-i) = i(-i) = 1.$$

Thus i and $-i$ both have order 4.

Solution to Exercise B143

(a) This group is abelian and has 7 elements of order 2, so it belongs to class 2. It is isomorphic to $S(\text{cuboid})$.

(b) This group is abelian and has exactly 3 elements of order 2, so it belongs to class 3. It is isomorphic to (U_{15}, \times_{15}) .

(c) This group is abelian and has only one element of order 2, so it belongs to class 1. It is isomorphic to $(\mathbb{Z}_8, +_8)$.

(Note also the bottom left to top right diagonal stripe pattern of the Cayley table: this shows that this group is cyclic.)

(d) This group is non-abelian and has only one element of order 2, so it belongs to class 5. It is isomorphic to the quaternion group Q_8 .

Solution to Exercise B144

(Hint for finding a solution to this exercise: Assume that A_4 has a subgroup H of order 6. By considering isomorphism classes, determine what the orders of the elements of H must be. Then show that H has a subgroup whose order does not divide 6.)

Suppose that A_4 has a subgroup H of order 6.

As A_4 has no element of order 6, H is isomorphic to the non-abelian group $S(\triangle)$. Thus H contains e , two elements of order 3 and three elements of order 2.

Now A_4 contains only three elements of order 2, namely

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3),$$

so these must all be in H . However, these three elements of order 2, along with e , form a subgroup of S_4 (it is the subgroup obtained by labelling the vertices of the rectangle with the symbols 1, 2, 3 and 4). This subgroup is a subgroup of H .

This subgroup has order 4, which contradicts Lagrange's Theorem, as 4 does not divide 6.

Thus A_4 has no subgroup of order 6.

(Here is an alternative solution, which you might have found. It starts in the same way as the solution above.

Suppose that A_4 has a subgroup H of order 6.

As A_4 has no element of order 6, H is isomorphic to the non-abelian group $S(\triangle)$. Thus H

contains e , two elements of order 3 and three elements of order 2.

Now A_4 contains only three elements of order 2, namely

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3),$$

so these must all be in H . Also, the two elements of order 3 in H must be inverses of each other, so they must be

$$(a\ b\ c) \quad \text{and} \quad (a\ c\ b),$$

for some distinct $a, b, c \in \{1, 2, 3, 4\}$. Let d be the element of $\{1, 2, 3, 4\}$ other than a, b and c . Then the permutation $(a\ b)(c\ d)$ is an element of H , since H contains all three possible permutations of this form. Thus, since H is a subgroup, the composite

$$(a\ b\ c) \circ (a\ b)(c\ d) = (a\ c\ d)$$

is also an element of H . This contradicts the fact that the only elements of order 3 in H are $(a\ b\ c)$ and $(a\ c\ b)$.

Thus A_4 has no subgroup of order 6.)

Solution to Exercise B145

(a) The hypothesis is

p is a prime number.

The conclusion is

$(\mathbb{Z}_p^*, \times_p)$ is a group.

(b) The theorem can be rephrased in the following forms.

(i) Let p be a prime number. Then $(\mathbb{Z}_p^*, \times_p)$ is a group.

(ii) $(\mathbb{Z}_p^*, \times_p)$ is a group whenever p is a prime number.

(iii) $(\mathbb{Z}_p^*, \times_p)$ is a group provided that p is a prime number.

(iv) p is a prime number only if $(\mathbb{Z}_p^*, \times_p)$ is a group.

(c) There is no definitively right or wrong answer as to which of (i)–(iv) in part (b) are good ways to state the theorem, but a reasonable answer is that (i)–(iii) are good ways, and (iv) is not, as it is less easy to understand.

Solution to Exercise B146

(a) The theorem can be rewritten as follows.

If n is an integer with $n \geq 2$, then the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n and is generated by the integer 1.

(b) The hypothesis is

- n is an integer with $n \geq 2$.

(Alternatively, you can regard the theorem as having two hypotheses:

- n is an integer,
- $n \geq 2$.)

The conclusions are

- the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n ,
- the group $(\mathbb{Z}_n, +_n)$ is generated by the integer 1.

Solution to Exercise B147

(a) The theorem can be written as

If G is a cyclic group, then G is abelian.

or

If a group is cyclic, then it is abelian.

(b) The converse can be stated as

If G is an abelian group, then G is cyclic.

or

If a group is abelian, then it is cyclic.

or

Every abelian group is cyclic.

(c) The converse is false. For example, $S(\square)$ is an abelian group that is not cyclic.

Solution to Exercise B148

(a) Statements 1, 3 and 6 are correct versions of the theorem.

(Statements 2 and 5 state the converse of the theorem, as mentioned in the solution to part (c) below, and statement 4 claims that in a group of even order *every* element has order 2, which is not what the original theorem claims.)

(b) There is no definitively right or wrong answer to this part, but a reasonable answer is that statements 1 and 6 are good ways to state the

theorem, and statement 3 is not, as it is less easy to understand.

(c) Statements 2 and 5 state the converse of the theorem.

(d) The converse is true, because the order of an element of a group divides the order of the group, by Corollary B69 to Lagrange's Theorem, so a group that contains an element of order 2 must have an order that is a multiple of 2.

Solution to Exercise B149

(a) Lemma B42 can be rephrased as an implication as follows.

If m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$ and m is a factor of n , then m has order n/m .

The hypotheses are

- m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$,
- m is a factor of n .

The conclusion is

- m has order n/m .

(Alternatively Lemma B42 can be regarded as having three hypotheses, as follows:

- m is an element of the group $(\mathbb{Z}_n, +_n)$,
- m is non-zero,
- m is a factor of n .

However, notice that if an element m of $(\mathbb{Z}_n, +_n)$ satisfies the hypothesis ' m is a factor of n ', then it must also satisfy the hypothesis ' m is non-zero'. So in fact the hypothesis ' m is non-zero' in Lemma B42 is not needed: the word 'non-zero' could be omitted from the statement of the lemma. It is included for convenience and clarity: it makes it immediately clear that the lemma applies only to non-zero elements of $(\mathbb{Z}_n, +_n)$.)

(b) Statements 1 and 3 are correct versions of Lemma B42, and statement 2 is incorrect.

(Statement 2 has ' m has order n/m ' as a hypothesis and ' m is a factor of n ' as a conclusion; they should be the other way round.)

Solution to Exercise B150

(a) The 'if' part of the theorem can be rephrased as an implication as

If G is a finite group of order n and G contains an element of order n , then G is cyclic,

or slightly more concisely as

If G is a finite group of order n that contains an element of order n , then G is cyclic.

The hypotheses are

- G is a finite group of order n ,
- G contains an element of order n .

The conclusion is

- G is cyclic.

(b) The 'only if' part of the theorem can be rephrased as an implication as

If G is a finite group of order n and G is cyclic, then G contains an element of order n ,

or slightly more concisely as

If G is a finite cyclic group of order n , then G contains an element of order n .

The hypotheses are

- G is a finite group of order n ,
- G is cyclic.

The conclusion is

- G contains an element of order n .

Solution to Exercise B151

(a) The 'if' part is as follows.

If $m \in \mathbb{Z}_n$ and m is coprime to n , then m is a generator of the group $(\mathbb{Z}_n, +_n)$.

The 'only if' part is as follows.

If $m \in \mathbb{Z}_n$ and m is a generator of the group $(\mathbb{Z}_n, +_n)$, then m is coprime to n .

(b) For the 'if' part, the hypotheses are

- $m \in \mathbb{Z}_n$,
- m is coprime to n .

The conclusion is

- m is a generator of the group $(\mathbb{Z}_n, +_n)$.

(c) For the ‘only if’ part, the hypotheses are

- $m \in \mathbb{Z}_n$,
- m is a generator of the group $(\mathbb{Z}_n, +_n)$.

The conclusion is

- m is coprime to n .

Solution to Exercise B152

The theorem can be written as:

If H is a subgroup of a cyclic group, then H is cyclic.

The contrapositive is:

If H is not cyclic, then H is not a subgroup of a cyclic group.

It can be stated more clearly as:

If a group is not cyclic, then it is not a subgroup of a cyclic group.

(It is possible to write the theorem in the form ‘If ..., then ...’ in a different way, and hence obtain its contrapositive in a different form. The theorem can alternatively be written as:

If G is a cyclic group, then every subgroup of G is cyclic.

The contrapositive of this statement is:

If it is not the case that every subgroup of G is cyclic, then G is not a cyclic group.

This can be stated more clearly as:

If a group G has a non-cyclic subgroup, then G is not a cyclic group.

Different ways of writing a theorem and its contrapositive can be useful in different situations.)

Solution to Exercise B153

Suppose that

$$a^2 = a.$$

Composing both sides on the left with a^{-1} gives

$$a^{-1}(a^2) = a^{-1}a.$$

Therefore

$$(a^{-1}a)a = a^{-1}a \quad (\text{by axiom G2, associativity}),$$

so

$$ea = e \quad (\text{by axiom G4, inverses}),$$

and hence

$$a = e \quad (\text{by axiom G3, identity}),$$

as required.

(Note that we could equally well have composed both sides on the *right* with a^{-1} here.)

Solution to Exercise B154

Suppose that

$$gh = e.$$

Composing both sides on the left with g^{-1} gives

$$g^{-1}(gh) = g^{-1}e.$$

Therefore

$$(g^{-1}g)h = g^{-1}e \quad (\text{by axiom G2, associativity}),$$

so

$$eh = g^{-1}e \quad (\text{by axiom G4, inverses}),$$

and hence

$$h = g^{-1} \quad (\text{by axiom G3, identity}),$$

as required.

Solution to Exercise B155

Suppose that

$$a^2 = a.$$

By axiom G3 (identity), this equation can be written as

$$aa = ae,$$

so, by the Left Cancellation Law,

$$a = e,$$

as required.

(Alternatively, we could have written the equation as $aa = ea$ and used the Right Cancellation Law.)

Solution to Exercise B156

Suppose that

$$gh = e.$$

By axiom G4 (inverses), this equation can be written as

$$gh = gg^{-1},$$

so, by the Left Cancellation Law,

$$h = g^{-1},$$

as required.

Solution to Exercise B157

Suppose that

$$abc = e.$$

Composing both sides on the left with a^{-1} gives

$$a^{-1}abc = a^{-1}e,$$

so

$$bc = a^{-1}.$$

Now composing both sides on the right with a gives

$$bca = a^{-1}a,$$

so

$$bca = e,$$

as required.

Solution to Exercise B158

Suppose that x and y commute. Then

$$xy = yx.$$

Composing both sides on the right with x^{-1} gives

$$xyx^{-1} = yxx^{-1},$$

that is,

$$xyx^{-1} = ye,$$

so

$$y = yxx^{-1},$$

as required.

(We compose on the *right* here because that gives xyx^{-1} on the left-hand side of the equation, which is the expression that we are trying to prove is equal to y . If instead we compose on the *left* with x^{-1} , then we obtain

$$x^{-1}xy = x^{-1}yx,$$

and hence

$$y = x^{-1}yx,$$

which is a different expression for y . This expression is also correct, but it is not the one we were asked to prove.)

Solution to Exercise B159

Two different proofs are given.

Proof 1

Since $(xy)^{-1}$ is the inverse of xy , we have

$$xy(xy)^{-1} = e.$$

Composing both sides with x^{-1} on the left gives

$$x^{-1}xy(xy)^{-1} = x^{-1}e,$$

that is,

$$y(xy)^{-1} = x^{-1}.$$

Now composing both sides with y^{-1} on the left gives

$$y^{-1}y(xy)^{-1} = y^{-1}x^{-1},$$

that is,

$$(xy)^{-1} = y^{-1}x^{-1},$$

as required.

Proof 2

We show that $y^{-1}x^{-1}$ is an inverse of xy . To do that, we have to show that

$$(xy)(y^{-1}x^{-1}) = e = (y^{-1}x^{-1})(xy).$$

Now

$$\begin{aligned} (xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} \\ &= xex^{-1} \\ &= xx^{-1} \\ &= e, \end{aligned}$$

and

$$\begin{aligned}(y^{-1}x^{-1})(xy) &= y^{-1}(x^{-1}x)y \\ &= y^{-1}ey \\ &= y^{-1}y \\ &= e,\end{aligned}$$

so $y^{-1}x^{-1}$ is an inverse of xy . Hence, since every group element has a unique inverse, $y^{-1}x^{-1}$ is *the* inverse of xy ; that is,

$$(xy)^{-1} = y^{-1}x^{-1}.$$

(This is the proof that you saw in Unit B1.)

Solution to Exercise B160

Two different proofs are given. The second uses Proposition B14.

Proof 1

Let g and h be any elements of G . We have to show that $gh = hg$.

Every element of G is self-inverse, so $gg = e$, $hh = e$ and

$$(gh)(gh) = e.$$

Composing both sides of the last equation on the left with g and on the right with h gives

$$g(gh)(gh)h = gh,$$

that is,

$$(gg)hg(hh) = gh,$$

which gives

$$ehge = gh.$$

Hence

$$hg = gh.$$

Thus G is abelian.

Proof 2

Let g and h be any elements of G . We have to show that $gh = hg$.

Every element of G is self-inverse, so $g^{-1} = g$, $h^{-1} = h$ and

$$(gh)^{-1} = gh.$$

By Proposition B14, we also have

$$(gh)^{-1} = h^{-1}g^{-1}.$$

Thus

$$gh = h^{-1}g^{-1}.$$

Therefore, since $g^{-1} = g$ and $h^{-1} = h$,

$$gh = hg.$$

Thus G is abelian.

Solution to Exercise B161

Let $P(n)$ be the statement

$$(x^n)^{-1} = (x^{-1})^n.$$

Then $P(1)$ is true, because the equation

$$(x^1)^{-1} = (x^{-1})^1$$

is equivalent to the equation

$$x^{-1} = x^{-1}.$$

Now let $k \geq 1$ and assume that $P(k)$ is true; that is,

$$(x^k)^{-1} = (x^{-1})^k.$$

We want to deduce that $P(k+1)$ is true, that is,

$$(x^{k+1})^{-1} = (x^{-1})^{k+1}.$$

Now

$$\begin{aligned}(x^{-1})^{k+1} &= (x^{-1})^k x^{-1} \\ &= (x^k)^{-1} x^{-1} \quad (\text{by } P(k)) \\ &= (xx^k)^{-1} \quad (\text{by Proposition B14}) \\ &= (x^{k+1})^{-1}.\end{aligned}$$

Hence $P(k+1)$ is true.

Thus $P(k) \implies P(k+1)$ for all $k \geq 1$. Therefore, by the Principle of Mathematical Induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Solution to Exercise B162

We know from Theorem B81 that $H \cap K$ is a subgroup of G , so $H \cap K$ is a group. Hence to prove that $H \cap K$ is a subgroup of H we just need to check that $H \cap K$ is a subset of H . This is true simply by the definition of $H \cap K$, so the stated result follows.

Solution to Exercise B163

We give a counterexample to the statement.

Let $G = S(\square)$, and take both H and K to be equal to G . Then H and K are subgroups of G and $H \cup K = G$, so $H \cup K$ is a subgroup of G . This counterexample shows that the given statement is not true.

(We could have taken G to be any group at all here, and there are also many other possibilities for H and K : we could have taken them both to be the trivial subgroup, for example, or we could have taken them to be any two equal subgroups.)

Solution to Exercise B164

We give a counterexample to the statement.

Let

$$\begin{aligned} G &= S(\square), \\ H &= \langle a \rangle = \{e, a, b, c\}, \\ K &= \langle b \rangle = \{e, b\}. \end{aligned}$$

Then H and K are distinct non-trivial proper subgroups of G . Also $H \cup K = H$, so $H \cup K$ is a subgroup of G . This counterexample shows that the given statement is false.

(We could have taken H and K to be any distinct non-trivial proper subgroups of a group G such that one of H and K is a subset of the other. Another such counterexample is obtained by taking G to be the cyclic group $(\mathbb{Z}_8, +_8)$ with $H = \langle 2 \rangle = \{0, 2, 4, 6\}$ and $K = \langle 4 \rangle = \{0, 4\}$.)

Solution to Exercise B165

We check that the three subgroup properties hold.

SG1 Let g and h be elements of $\langle x \rangle$. Then $g = x^s$ and $h = x^t$ for some integers s and t . So

$$gh = x^s x^t = x^{s+t}.$$

Since $s + t \in \mathbb{Z}$, this shows that gh can be written as a power of x , so $gh \in \langle x \rangle$.

SG2 The identity element e of G can be written as $e = x^0$, so it is in $\langle x \rangle$.

SG3 Let g be any element of $\langle x \rangle$. Then $g = x^s$ for

some integer s . Now

$$\begin{aligned} g^{-1} &= (x^s)^{-1} \\ &= x^{-s} \quad (\text{by one of the index laws}). \end{aligned}$$

Since $-s \in \mathbb{Z}$, this shows that g^{-1} can be written as a power of x , so $g^{-1} \in \langle x \rangle$.

Since all three subgroup properties hold, $\langle x \rangle$ is a subgroup of G .

Solution to Exercise B166

We know that K is a subgroup of H , so K is a group. Hence to prove that K is a subgroup of G we just need to check that it is a subset of G . This is true because K is a subset of H and H is a subset of G . Hence K is a subgroup of G .

Solution to Exercise B167

Let G be an abelian group, and let H be a subgroup of G .

Let $x, y \in H$. Then $x, y \in G$ since H is a subgroup of G . Since G is abelian, it follows that $xy = yx$. Thus H is abelian, as required.

Solution to Exercise B168

Let the order of H and K be p , where p is prime. By Theorem B81, the set $H \cap K$ is a subgroup of G . It is also a subset of each of H and K , so it is a subgroup of each of H and K . Hence, by Lagrange's Theorem, its order divides p , so it is either 1 or p . If it is p , then $H \cap K$ is a subgroup of H that has the same order as H , so $H \cap K = H$, and similarly $H \cap K = K$. But this is impossible since $H \neq K$. Hence the order of $H \cap K$ is 1, and therefore, since $H \cap K$ is a subgroup, $H \cap K = \{e\}$.

Solution to Exercise B169

Let the orders of H and K be p and q , respectively, where p and q are coprime. By Theorem B81, the set $H \cap K$ is a subgroup of G . It is also a subset of each of H and K , so it is a subgroup of each of H and K . Hence, by Lagrange's Theorem, its order divides p and q . Since p and q are coprime, their only positive common factor is 1, so the order of $H \cap K$ is 1. Therefore, since $H \cap K$ is a subgroup, $H \cap K = \{e\}$.

Solution to Exercise B170

Attempt 3

This attempted proof is incorrect. It gives an *example* of a group of even order that contains an element of order 2, but to prove the theorem we have to prove that *every* group of even order contains an element of order 2.

(This kind of 'proof' is known to mathematics tutors as a 'proof by example'; this is not a valid method of proof!)

Attempt 4

This attempted proof is also incorrect. It is a correct proof of the following statement:

A group that contains an element of order 2 has even order.

This is the *converse* of the theorem to be proved. Unfortunately the fact that the converse of a statement is true tells us nothing about the truth of the original statement.

(The solution to Worked Exercise B56, Attempt 2, gives another way of expressing the converse – that way is the contrapositive of the statement above.)

Attempt 5

This attempted proof is correct. It correctly proves the contrapositive of the theorem to be proved, and the contrapositive is equivalent to the theorem.

(However, the proof would have been clearer if it had started by saying that it was going to prove the contrapositive and had then stated the contrapositive.)

Attempt 6

This attempted proof is incorrect. The problem occurs in the step 'Then there is no element x of G that satisfies the equation $x^2 = e$.' This is not a correct deduction, because even if a group does not contain an element of order 2, there is still an element x of G that satisfies the equation $x^2 = e$, namely the identity element e .

(Saying that an element x has order 2 is not *equivalent* to saying that $x^2 = e$. If an element x has order 2, then it follows that $x^2 = e$, but if an element x satisfies $x^2 = e$ then it does not follow that it has order 2, as x could be e , which has order 1.)

Solution to Exercise B171

(a) The problem is that to show that the order of ba is n , we have to show not only that $(ba)^n = e$, but also that there is no natural number k smaller than n such that $(ba)^k = e$.

(b) We can fix the proof by adding the following immediately before the sentence 'Hence ba also has order n .'

Now suppose that there is a natural number k smaller than n such that

$$(ba)^k = e.$$

Then, by an argument similar to the one above, it follows that

$$(ab)^k = e.$$

But this contradicts the fact that the order of ab is n . So there is no such natural number k .

Alternatively, we can exploit the fact that the elements a and b in the original statement are interchangeable, and replace the sentence 'Hence ba also has order n .' by the following.

Let the order of ba be m . Then the argument above shows that $m \leq n$. By the same argument, with the roles of a and b interchanged, it follows that the order of ab is at most m ; that is, $n \leq m$.

Since $m \leq n$ and $n \leq m$, we have $m = n$.

There are other possibilities for fixing the proof, apart from the two suggestions above.

Acknowledgements

Grateful acknowledgement is made to the following sources.

Cover image: © Mark Owen

Unit B1

Évariste Galois (Subsection 3.1): Portrait of Évariste Galois. Artist unknown

Unit B2

Camille Jordan (Subsection 4.2): Archives Charmet / Bridgeman Art Library / Universal Images Group

Felix Klein (Subsection 4.2): Felix Christian Klein. Photographer unknown

Unit B3

Augustin-Louis Cauchy (Subsection 1.1): Augustin-Louis Cauchy taken in 1901. Photographer unknown

Joseph-Louis Lagrange (Subsection 1.3): © Georgios Kollidas / 123RF

William Burnside (Subsection 2.1): William Burnside. Photographer unknown

Church bells (Subsection 2.4): Courtesy of Johnathon Frye

Bell ringers (Subsection 2.4): © Robert Smith / Alamy Stock Photo

Unit B4

William Rowan Hamilton (Subsection 2.5): William Rowan Hamilton. Image in the public domain

Brougham Bridge (Subsection 2.5): From: Ingenious Ireland. Hamilton Quaternions walk 2011

Paul Erdős (Subsection 3.2): Kmhkmh. This file is licensed under the Creative Commons Attribution 3.0 Unported licence.

<https://creativecommons.org/licenses/by/3.0/deed.en>

Alfred Bray Kempe (Subsection 3.5): Taken from www.maa.org

Appel and Haken (Subsection 3.5): University of Illinois Board of Trustees

Henri Poincaré (Subsection 3.5): Library of Congress / Science Photo Library / Universal Images Group

Andrew Wiles (Subsection 3.5): Klaus Barner. This file is licensed under the Creative Commons Attribution-Share Alike Licence

<http://creativecommons.org/licenses/by-sa/3.0/>

Every effort has been made to contact copyright holders. If any have been inadvertently overlooked the publishers will be pleased to make the necessary arrangements at the first opportunity.

Index

- A_4 246
- A_n *see* alternating group
- abelian (commutative) group 35, 69
- abstract group 295, 303
 - notation convention for 303
- additive group 131
- additive identity 36
- additive inverse 36
- additive notation 131
- alternating group A_n 245
 - degree of 245
 - order of 247
- angle of rotation 6, 72
 - clockwise/anticlockwise 6
- Appel, Kenneth 342
- associative binary operations 38
- associativity 15, 34, 53
- axioms for a group 331
- axis of symmetry 4, 72

- bell ringing 233
- Bhāskara II 219
- binary operation 33
 - unfamiliar 43, 117
- body of a Cayley table 47
- border of a Cayley table 47
- bounded figure 5, 70
- Burnside, William 220

- Cancellation Laws 65, 333
- Cauchy, Augustin-Louis 211
- Cayley, Arthur 273
- Cayley table 30, 46
 - borders and body of 47
 - main diagonal of 47
 - of a group of order four 165
 - of a group of order six 166
 - using to check group axioms 52
- Cayley's Theorem 271
 - proof of 274
- centre of rotation 6
- closure 11, 34
- commutative (abelian) group 35, 69
- commutativity 14, 35
- commuting elements 336
- composite of permutations 212–214
- concise multiplicative notation 304
- conclusion of a theorem 320, 323
- congruent figures 71
- conjugate 254, 255
- conjugate permutation 254, 255
- conjugate subgroup 259
 - finding 260
- conjugating permutation 254
 - finding 256
- contrapositive 327
- converse 324
- convex polyhedron 71
- corollary 322
- coset 298
- cube 71
- cuboid, symmetry group of 87
- cycle 206, 222
 - as a composite of transpositions 237
 - disjoint 208
 - length of 222
 - order of 224
 - parity of 240
- cycle form of a permutation 208
 - conventions for 211
 - finding 209
 - uniqueness of 210
- cycle number of a permutation 248
- cycle of powers/multiples of an element 139
- cycle structure 222
 - of permutations in S_3 223
 - of permutations in S_4 223, 262
 - of permutations in S_5 223
- cyclic group 149, 185
 - finite 149
 - from modular arithmetic 153, 154
 - subgroups of 150
- cyclic subgroup 143
 - generator of 143

- dihedral group 312
- direct symmetries, group of 122
- direct symmetry 20, 21, 75
- disc, symmetries of 18, 147
- disjoint cycles 208
 - product of 208
- divisor of an integer 294

- dodecahedron 71, 79, 88
- double tetrahedron 230
- equilateral triangle 7
 - Cayley table of symmetries of 31
 - symmetries of 15, 27
- equivalence of statements 326
- Erdős, Paul 330
- even permutation 240
- factorial 221
- field 36
- figure 5, 70
 - fixing a vertex or edge of 124
 - modifying 122
- finite group 35
- finite group of numbers 114
- fixed symbol 210
- generator 143
 - of $(\mathbb{Z}_n, +_n)$ 156
 - of a cyclic group/subgroup 143
- glide-reflection 6
- group 34
 - abelian/non-abelian 35, 69
 - abstract 295
 - additive 131
 - axioms 108
 - cyclic/non-cyclic 149
 - finite/infinite 35
 - isomorphic 169
 - multiplicative 131
 - of order 4 308–309
 - of order 6 309–312
 - of order 8 313–315
 - of numbers, standard 114
 - of prime order 300–302
 - order of 35, 293
- group axioms 34, 331
 - checking 36–46
 - checking for small sets 46–52
 - deductions from 59–66
- group table 66
 - properties 66–69
- Haken, Wolfgang 342
- Hamilton, William Rowan 316
- Heawood, Percy John 342
- hexagon 7, 27
- hypothesis of a theorem 320, 323
- icosahedron 71, 79, 88
- identity element (identity) 6, 34, 49, 61, 67, 108
 - additive 36
 - in a subgroup 111
 - multiplicative 36
 - order of 135
 - subgroup generated by 144
- identity permutation 211
- identity symmetry 6, 16
- identity transformation 6, 72
- implication 320
- index laws for group elements 130
 - in additive notation 132
- indirect symmetry 20, 21, 75
- induction, proof by 337
- infinite group 35
- infinite group of numbers 114
- infinite order 35
- inverse element (inverse) 34, 50, 62
 - additive 36
 - in a subgroup 111
 - multiplicative 36
 - of a 2-line symbol 29
 - of a composite 63
 - of a permutation 217–218
 - of a symmetry 17, 29–30
 - of an inverse 63
 - order of 135
- isometry 5, 72
- isomorphic groups 169
 - properties of 170, 178
 - strategies for identifying 174, 181, 184
- isomorphism 169
 - as an equivalence relation 170
 - finding 171, 174, 184
 - of cyclic groups 183
 - properties of 175–180
- isomorphism class 170, 302
 - for groups of order 4 309
 - for groups of order 6 312
 - for groups of order 8 315
 - for groups of orders 1 to 8 318
 - for groups of prime order 302, 307
- Jordan, Camille 169, 245
- juxtaposition 217

- Kempe, Alfred Bray 342
- Klein four-group, V 171, 308
- Klein, Felix 171
- Lagrange's Theorem 294
 - corollaries of 300
- Lagrange, Joseph-Louis 219, 299
- leading diagonal 47
- least common multiple 225
- Left Cancellation Law 65
- lemma 325
- length of a cycle 222
- main diagonal (of a Cayley table) 47
- modifying a figure 122
- modular arithmetic 46
 - groups from 56
- multiple, in an additive group 131
- multiplicative group 131
- multiplicative identity 36
- multiplicative inverse 36
- multiplicative notation 131
 - concise 304
- n -gon (polygon) 7, 10
- non-abelian group 35
- non-cyclic group 149
- notation convention for abstract groups 303
- notation, multiplicative/additive 131
- octahedron 71, 79, 88
- odd permutation 240
- order
 - of a group 35
 - of a group element 133, 300
 - finite/infinite 133
 - in $(\mathbb{Z}_n, +_n)$ 155
 - of a permutation 224
 - finding 225
 - of a subgroup 293
- paper model of a plane figure 7
- parity 240
 - of a cycle 240
 - of a permutation 240
 - finding 242–244
- Parity Theorem 240
 - proof of 247
- pentagonal prism 79
- permutation 205
 - as a composite of transpositions 238
 - composing 212–214
 - conjugating 254, 256
 - cycle form of 208, 209
 - cycle number of 248
 - even/odd 240
 - inverse of 217–218
 - order of 224
 - parity of 240
 - two-line form of 206
- permutation group 222
 - representing a group as 227, 271
- plane figure 5
- plane of reflection 72
- Platonic solid 71, 88
- Poincaré, Henri 343
- polygon (n -gon) 7
 - symmetries of 10, 26
- polyhedron 70
 - convex 71
 - finding the symmetries of 84
 - number of symmetries of 79, 82
 - regular 71
- power of a group element 129, 136
- prime order, group of 300–302
- prism 79
- product
 - of disjoint cycles 208
 - of permutations 217, *see also* composite of permutations
- proof
 - checking 342
 - producing 329
- proper subgroup 110, 302
- proposition 320
- Q_8 (quaternion group) 314
- quaternions (history) 316
- \mathbb{R}^+ 115
- rectangle
 - symmetries of 15
- reflection 6, 72
- reflectional symmetry 6
- regular polygon (n -gon) 7
 - symmetries of 10

- regular polyhedron 71
 - number of symmetries of 79
- rhombicuboctahedron, small 81
- Right Cancellation Law 65
- rotation 6, 72
 - trivial/non-trivial 7
- rotational symmetry 6

- $S(\triangle)$ 31
- $S(\square)$ 31
 - subgroups of 293
- $S(\square)$ 32
- $S(\circ)$, cyclic subgroups of 147
- $S(\text{tet})$ 267
 - subgroups of 125, 267
- $S(F)$ 11
- $S^+(F)$ 20, 76, 122
- S_4 223
 - subgroups of 261, 266, 294
- S_n *see* symmetric group
- self-inverse element 17, 50
 - order of 135
 - subgroup generated by 144
- small rhombicuboctahedron 81
- solid (solid figure) 70
- square 7
 - Cayley table of symmetries of 31
 - composing symmetries of 11–13
 - direct/indirect symmetries of 21
 - paper model of 7
 - symmetries of 8–9
 - two-line symbols for 27
- standard groups of numbers 114
 - finite 56–58
 - infinite 55
- subgroup 109, 337
 - checking 112
 - conjugate 259
 - cyclic 143
 - finding 267
 - generated by an element 141, 143
 - of $(\mathbb{Z}_n, +_n)$ 158
 - of $S(\square)$ 293
 - of S_4 261, 266, 294
 - of a symmetry group 127
 - order of 293
 - proper 110, 302
 - trivial 110
- subgroup properties 112
- subgroup test 338
- symbols being permuted 206
- symmetric group S_n 220
 - degree of 220
 - order of 221
- symmetry group (of a figure) 75
 - finding subgroups of 127
 - subgroup of direct symmetries of 122
- symmetry of a figure 5, 72
 - composing 12–13, 27–28, 74
 - equality of 7, 72
 - identity (trivial) 6
 - representing as a permutation 227
- tetrahedron 71, 88
 - number of symmetries of 77–78
 - symmetries of 84–87
 - symmetry group of 267
 - subgroups of 125
- translation 6
- transposition 222
- triangular prism 83, 127
- trivial rotation 7
- trivial subgroup 110
- trivial symmetry 6
- two-line form of a permutation 206
- two-line symbol for a symmetry 24, 26, 73
 - composing 28
 - inverting 29

- (U_n, \times_n) 57, 154
- U_n 56
- uniqueness properties 61–62

- V (Klein four-group) 171, 308

- Wiles, Andrew 343
- 4-windmill 9
 - symmetries of 15

- \mathbb{Z}^+ 116
- $(\mathbb{Z}_n, +_n)$ 56, 153, 155
 - generators of 156
 - order of an element of 155
 - subgroups of 158
- $(\mathbb{Z}_p^*, \times_p)$ 58

